ACQUEDOTTO POIANA S.P.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

redatto ai sensi del D.Lgs. 231 dell'8 giugno 2001 e ss.mm.ii.

PARTE SPECIALE

REATI INFORMATICI, VIOLAZIONI IN MATERIA DI DIRITTO D'AUTORE E IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI. REATI CONTRO LA PERSONALITÀ INDIVIDUALE

Versione	12
Dirigente delegato	Direttore Generale
Organo di approvazione	Consiglio di Amministrazione
Data di approvazione	28 gennaio 2026

INDICE

1 PREMESSA 1
2 LE FATTISPECIE DI REATO CONTEMPLATE NELLA PRESENTE PARTE SPECIALE 2
2.1 Reati in materia di delitti informatici e trattamento illecito dei dati. 5
2.2 Delitti contro la personalità individuale 19
2.3 Delitti in materia di strumenti di pagamento diversi dai contanti 22
2.4 Delitti in materia di violazione del diritto di autore 25
2.5 Delitti contro la Dignità e Personalità Individuale 30
3 SANZIONI. 31
4 ESCLUSIONE DELLA RESPONSABILITÀ AMMINISTRATIVA 35
LA REALTA' CONSIDERATA 36
LE ATTIVITÀ "SENSIBILI" AI FINI DEL D.LGS. 231/01. SOGGETTI COINVOLTI E DESTINATARI DELLA PRESENTE PARTE SPECIALE 36
5 IL SISTEMA DEI CONTROLLI 45
5.1 Valori condivisi: il Codice Etico. 46
5.2 Protezioni Hardware e Software 47
5.3 La Policy sul trattamento dati e sull'utilizzo degli strumenti 48
6 INTERAZIONE CON ALTRI REATI PRESUPPOSTO 55
7.1 Reati di cui all'art. 24 D.Lgs. 231/01 55
7.2 Reati di cui all'art. 25 D.Lgs. 231/01 55
7.3 Reati di cui all'art. 25 ter D.Lgs. 231/01 56
7.4 Reati di cui all'art. 25 octies D.Lgs. 231/01 56
7.5 Reati di cui all'art. 25 decies D.Lgs. 231/01 56
7.6 Reati di cui all'art. 25 undecies D.Lgs. 231/01 56
7.7 Reati di cui all'art. 25 quinquiesdecies D.Lgs. 231/01 57
8. Documentazione aziendale di riferimento 57

1 PREMESSA

La presente Sezione costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo di cui Acquedotto Poiana s.p.a. (di seguito, per semplicità, anche solo "*Poiana*" o la "*Società*") si è dotata al fine di adempiere alle previsioni del D.Lgs. n. 231 del 08.06.2001 (di seguito per brevità anche il "*Decreto*"), in relazione ai reati previsti dagli **artt. 24** e **25 *quinqiues*** del D.Lgs. n. 231/2001.

Tutti i destinatari del Modello, così come individuati nella Parte Generale e nella presente Parte Speciale, sono chiamati all'osservanza dei principi e delle linee di condotta indicati di seguito, nonché ad adottare, ciascuno in relazione alla funzione in concreto esercitata, comportamenti conformi ad ogni altra norma e/o procedura che regoli in qualsiasi modo attività che rientrano nell'ambito di applicazione del D.Lgs. n. 231/2001 quanto alle fattispecie di reato trattate nella presente Parte Speciale.

L'adozione da parte di Poiana di un Modello di Organizzazione, Gestione e Controllo in grado di prevenire adeguatamente le differenti ipotesi di illecito previste da tale normativa da parte dell'Ente, trova il proprio presupposto fondamentale nella volontà di pianificare *ex ante* le misure di risposta ai reati in un'ottica integrata che consente di gestire la propria infrastruttura informatica ed i propri archivi, sia affrontando la questione con misure tecniche coordinate, che attraverso l'adozione di regole e procedure alla cui osservanza sono tenuti tutti gli Amministratori, Dirigenti, Lavoratori, Collaboratori esterni a qualsiasi titolo e chiunque svolga, a qualsiasi titolo, funzioni di rappresentanza anche di mero fatto di Poiana.

L'adozione di protocolli *ex* D.Lgs. n. 231/01, peraltro, deve necessariamente coordinarsi anche con altri ambiti normativi cui l'Ente è tenuto e che impongono l'adozione di misure di sicurezza tecniche, organizzative e procedurali tra cui, in particolare, il Reg. UE 2016/679 (c.d. "GDPR") e i provvedimenti dell'Autorità Garante in materia di Trattamento dei Dati Personali[1].

Al fine di creare un sistema organico di comportamenti, Acquedotto Poiana s.p.a. ha adottato (ed aggiornato) specifiche procedure e misure operative, finalizzate a garantire, da un lato, una gestione ed un utilizzo lecito e sicuro del proprio sistema informatico e, dall'altro, una gestione conforme ai dettami normativi e dispositivi in materia di trattamento dei dati.

Ciò premesso si evidenzia che sono tre i requisiti da cui dipende la possibilità di imputare all'Ente collettivo un illecito dipendente da reato: **1)** la commissione di una delle fattispecie di reato indicate negli artt. 24-26 del D.Lgs n. 231/2001); **2)** l'autore di tale reato sia una persona fisica appartenente ad una certa categoria di soggetti [in particolare: *a*) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'Ente stesso - art. 5, 1° co., lett. a) del Decreto *b***)** persone sottoposte alla direzione o alla vigilanza di uno di costoro - art. 5, 1° co., lett. b) del Decreto]; **3)** il reato, inoltre, deve essere stato commesso nell'interesse o a vantaggio dell'Ente.

Elemento costitutivo della responsabilità dell'Ente – caratterizzata dalla c.d. "*colpa di organizzazione*" - è che la condotta illecita sia stata posta in essere *"nell'interesse o a vantaggio della Società*" e non *"nell'interesse esclusivo proprio o di terzi"* (art. 5, comma 1 e 2 del Decreto).

[1] https://www.garanteprivacy.it/

Ne deriva che la responsabilità dell'Ente sorge non soltanto allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno, per l'Ente, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'interesse dell'Ente.
L'art. 12, primo comma, lett. a) del Decreto, stabilisce una riduzione della sanzione pecuniaria per il caso in cui *"l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricevuto vantaggio minimo":* pertanto anche se il soggetto ha agito perseguendo sia l'interesse proprio che quello dell'Ente, quest'ultimo sarà passibile di sanzione.
Ove risulti prevalente l'interesse dell'agente rispetto a quello dell'Ente, sarà possibile un'attenuazione della sanzione stessa a condizione, però, che l'Ente non abbia tratto vantaggio o abbia tratto vantaggio minimo dalla commissione dell'illecito.
Nel caso in cui, invece, l'autore del reato-presupposto sia un sottoposto [lett. *b*) dell'art. 5, 1° co. del Decreto] l'Ente sarà responsabile *«se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza»*: e tuttavia, è previsto che tale inosservanza debba ritenersi esclusa nel caso in cui *«l'Ente, prima della commissione del reato, "avesse" adottato un modello di organizzazione, gestione o controllo idoneo a prevenire reati della specie di quello verificatosi»* (art. 7, 1° e 2° comma, del D.Lgs n. 231/2001).
Peraltro, pur essendo dipendente dalla commissione di un reato da parte di una persona fisica, la responsabilità da reato dell'Ente collettivo è in certo senso autonoma da quella penale dell'autore del reato-presupposto (art. 8 del D.Lgs. n. 231/2001): essa, infatti, non è esclusa dal fatto che l'autore del reato-presupposto non venga identificato o non sia imputabile, né viene meno nel caso in cui il reato-presupposto si estingua per causa diversa dall'amnistia.

2 LE FATTISPECIE DI REATO CONTEMPLATE NELLA PRESENTE PARTE SPECIALE

L'art. 7 della Legge n. 48/2018, mediante l'inserimento nell'ambito del D.Lgs. n. 231/2001 dell'**art. 24 *bis*** sui delitti informatici e trattamento illecito dei dati, ha introdotto fattispecie di reato che possono generare una responsabilità amministrativa in capo alla Società: si tratta dei reati cosiddetti "informatici", dei quali ci si occuperà nel prosieguo della presente Parte Speciale, ma si anticipa sin d'ora che gli strumenti informatici possono essere utilizzati anche per commettere reati appartenenti ad altre fattispecie (reati informatici come "mezzo" per commettere altri reati).
Di qui, la necessità di esaminare anche altre tipologie di reati presupposto e di prevenire questi ultimi mediante l'adozione di misure tecniche, organizzative (legate, cioè all'introduzione di funzioni gerarchiche ed all'attribuzione di ruoli e mansioni, nonché del rafforzamento di competenze hard/soft) e procedurali, che intervengono sulle modalità attuative dei reati con l'utilizzo di strumenti informatici.
Proprio per questa peculiarità, si è ritenuto di dover trattare qui anche reati presupposto che non rientrano solo nell'ambito di cui al citato **art. 24 *bis***.
Per meglio comprenderne la natura, vengono riportati i testi anche degli **artt. 24** e **25 *quinquies*** del D.Lgs. n. 231/2001[2]:

Art. 24

[2] Con riferimento a questa Parte Speciale, il D.Lgs. 231/01 è stato modificato: dal D.L. 10/08/2023 n. 105 conv. con L. 137 del 9/10/2023 per quanto riguarda l'art. 24; dal D.L. 21/09/2019 n. 105 conv. con L. 133 del 18/11/2019 per quanto riguarda l'art. 24 bis; dalla L. 29/10/2016, n. 199 per ciò che attiene l'art. 25-quinquies; il D.Lgs. 7/7/2011, n. 121 per quanto concerne l'art. 25-novies.

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

In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 353, 353-bis, 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 entità o è derivato un danno di particolare gravità; 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).

Art. 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 da duecento a settecento quote.

1- bis. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 635 -quater .1 del codice penale, si applica all'ente la sanzione pecuniaria sino a quattrocento 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 per i 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[3], 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 il delitto indicato nel comma 1 -bis si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni

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).

Art. 25-quinquies
Delitti contro la personalità 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, 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, la sanzione pecuniaria da duecento a settecento quote.

[3] Il D.L. 21/09/2019 n. 105 "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"* è stato convertito, con modifiche, dalla L. 18 novembre 2019, n. 133 ed è stato oggetto di diverse modifiche. L'intento del Legislatore è di normare in maniera diversa e tutelare maggiormente settori e contesti speciali.

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.

Gli strumenti informatici, nella prassi, vengono sovente utilizzati anche per commettere reati appartenenti ad altre fattispecie (reati informatici come "mezzo" per commettere altri reati) e quindi la presente Parte Speciale può e deve essere considerata – in linea di principio – come integrante di per sé gli altri elaborati del Modello (ed in primis la *Policy Whistleblowing* di Poiana).
Ed è quindi ineludibile prevenire la commissione dei reati presupposto della responsabilità amministrativa degli Enti anche mediante l'adozione di misure tecniche, organizzative (legate, cioè all'introduzione di funzioni gerarchiche ed all'attribuzione di ruoli e mansioni, nonché del rafforzamento di competenze hard/soft) e procedurali che intervengono sulle modalità attuative dei reati con l'utilizzo di strumenti informatici.
Sussiste, peraltro, un nesso oggettivo fra gli strumenti ed i reati informatici e le fattispecie di cui agli **artt. 25 *octies.1*** (*in materia di strumenti di pagamento diversi dai contanti*) e **25 *novies*** (*in materia di violazione del diritto d'autore*) del D.Lgs. n. 231/2021:

Art. 25-octies.1
Delitti in materia di strumenti di pagamento diversi dai contanti

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.
c) per il delitto di cui all'articolo512-bis, la sanzione pecuniaria da 250 a 600 quote.
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.
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.

Art. 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.

Di seguito, trovano spazio le norme che disciplinano i reati informatici ed i reati collegati al trattamento illecito dei dati.

2.1 Reati in materia di delitti informatici e trattamento illecito dei dati.

Nel caso particolare degli strumenti informatici, come precedentemente evidenziato, questi ultimi possono costituire sia un mezzo di compimento di reati presupposto, sia uno strumento per il compimento di reati presupposto di altra natura.
È importante, quindi, riflettere su entrambi gli ambiti e, nel prosieguo, saranno presentati riferimenti normativi in queste due accezioni.

2.1.1 Reati propriamente informatici citati nell'art. 24 *bis* D.lgs. 231/01

Di seguito si riporta il testo degli articoli del Codice Penale che descrivono i reati "presupposto" della responsabilità amministrativa dell'Ente specificatamente indicati nell'art. 24 *bis* D.lgs. n. 231/2001 in relazione ai delitti informatici ed al trattamento illecito dei dati.

Il presente Modello è stato aggiornato in conformità alle disposizioni introdotte dalla **Legge 28 giugno 2024, n. 90**, recante *«Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici»*.
In particolare, la Società prende atto del sensibile inasprimento del quadro sanzionatorio per i delitti di cui agli artt. 615-ter, 617-quater, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, nonché dell'introduzione della nuova fattispecie di cui all'**art. 629, comma 3, c.p.** (estorsione mediante reati informatici). Quest'ultima configura un nuovo e rilevante reato presupposto ai sensi del D.Lgs. 231/2001, per il quale l'Ente ha adeguato i propri protocolli di prevenzione e i sistemi di monitoraggio degli accessi logici, al fine di mitigare il rischio di condotte estorsive attuate tramite attacchi ransomware o danneggiamento di sistemi informativi.

Art. 615 ter
Accesso abusivo ad un sistema informatico o telematico

1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione da due a dieci anni
2. La pena è della reclusione da due a dieci anni:
1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare del sistema dei dati, delle informazioni o dei programmi in esso contenuti.
3. Qualora i fatti di cui al comma primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla

protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni.
4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Questa articolata fattispecie di reato è stata introdotta dalla Legge n. 547/93 e poi da ultimo modificata con la Legge n. 90 del 28/06/2024.
Essa si configura come un delitto comune, dato che è possibile la sua commissione da parte di "*chiunque*", e come reato "*istantaneo*" poichè la sua consumazione avviene nel momento dell'introduzione o nella protrazione all'interno del sistema nonostante il dissenso del titolare dello *ius excludendi*. Infatti, il reato incrimina due differenti condotte:

- l'introduzione abusiva in un sistema protetto;
- l'atto di mantenersi nel sistema contro la volontà del titolare del diritto.

Quanto alla prima condotta, ancora discusso è il perimetro interpretativo delle definizioni di *"abusivamente*" e di "*protezione attraverso misure di sicurezza"* del sistema violato.
La natura abusiva va ricondotta alla esplicita volontà del titolare di escludere qualcuno da un sistema[4], mentre per protezione si intendono misure che si sostanziano in un qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico. Tali misure possono essere di tipo hardware o software (misure logiche) ma anche essere costituite da strumenti esterni al sistema (protezione fisica) o meramente organizzativi, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi.
Per questo reato è punibile anche il solo tentativo: ad esempio, viene punito chi, forzando la serratura, si introduce nei locali di un'impresa fornitrice adibiti alla "programmazione" per sottrarre know-how anche se, prima della commissione, il suo tentativo viene sventato grazie all'arrivo della vigilanza, nonostante i sistemi informatici/telematici oggetto materiale della violazione non siano protetti da misure di sicurezza logiche.
La seconda condotta presa in considerazione dalla norma in esame è quella di colui che "*si mantiene*" all'interno del sistema "*contro la volontà esplicita o tacita di chi ha il diritto di escluderlo*".
Quindi nel caso in cui un soggetto possa "*legittimamente introdursi*", ma il suo intervento debba essere limitato a determinate operazioni, nel momento in cui si oltrepassano i limiti della propria competenza (in termini di incarico ricevuto, per ambito dei dati ed operazioni eseguite sugli stessi), o delle finalità consentite risulta integrato il reato in commento [5].
La fattispecie di reato in commento risulta integrata anche prendendo visione di dati per semplice curiosità: non sono, infatti, ritenuti rilevanti gli scopi e le finalità soggettivamente perseguiti da chi commette il reato, così come non è rilevante l'effettivo impiego successivo dei dati ottenuti.
Altri esempi di condotte integranti il reato in commento sono:

[4] Così la Corte di Cassazione Penale, sezione V, nella sentenza n. 15629/2022: peraltro tale orientamento afferma che "*integra il delitto previsto dall'art. 615-ter c.p. la condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema*", così postulando un duplice stato dell'abusività per cui, con riferimento agli insider privati, assumerebbe rilievo il solo abuso oggettivo dell'accesso o della permanenza nel sistema informatico, mentre per i pubblici funzionari, l'alveo del delitto di accesso abusivo a sistema informatico parrebbe più ampio, ricomprendendo ogni abuso del titolo, anche soggettivo.

[5] Al riguardo si segnalano le sentenze della Corte di Cassazione Penale, sez. V, n. 2457/2021 e n. 1161/2024, in merito ad appartenenti alla polizia giudiziaria ritenuti accessi abusivi in quanto avvenuti per finalità estranee a quelle proprie dell'ufficio

- l'alterazione del funzionamento di alcune caselle vocali riservate ai dipendenti di una società e programmate in modo che partano telefonate a ciclo continuo dal numero del gestore verso le utenze mobili prepagate con il profilo "autoricarica";
- l'introduzione da parte di un soggetto che, pur avendo titolo e formale legittimazione per accedere al sistema stesso, vi si introduca su istigazione criminosa di un terzo nel contesto di un accordo di corruzione, ad esempio, per falsare i risultati di un referto analitico;
- la modifica, ad opera di un addetto al sistema operativo di alcune situazioni contributive e debitorie, riducendo il debito o aumentando il credito.

Art. 615 quater
Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

Chiunque, al fine di procurare a sé o ad altri un vantaggio 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 al predetto scopo, è punito reclusione ***fino a due anni e multa fino a 10.329 euro****. Se il fatto è commesso a danno di sistemi di interesse pubblico o da operatori del sistema, la pena è della reclusione* ***da uno a cinque anni****.*

Per comprendere questo reato, è necessario che si precisino alcuni termini:

- per "*diffusione*" si intende il mettere a conoscenza di una o più persone indeterminate i codici di accesso, in qualunque forma, attraverso la disponibilità degli stessi (anche attraverso pubblicazione su un sito Internet);
- per "*riproduzione*" si intende la produzione di una copia abusiva di un codice, di una "parola chiave" o di ogni altro mezzo idoneo all'accesso;
- per "*consegna*" va intesa la cessione materiale delle credenziali di accesso a un determinato soggetto;
- per "*comunicazione*" si intende il mettere a conoscenza di una o più persone determinate dei codici di accesso.

La fattispecie in commento – anch'essa modificata dalla citata Legge n. 90/2024 - è un reato comune (quindi che chiunque può commettere), di pericolo (non richiede che l'evento lesivo si realizzi effettivamente), istantaneo e richiede, come elemento soggettivo, il dolo specifico, ossia il fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno.
Anche in questo caso la norma richiede che il sistema informatico/telematico sia protetto da misure di sicurezza costituite da barriere fisiche o virtuali e, grazie alla locuzione "*altri mezzi idonei all'accesso*", il legislatore, ha cercato di renderla applicabile anche a fattispecie, al momento, non prevedibili.

Art. 617 quater
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrente fra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
2. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
3. I delitti di cui al comma primo e secondo sono punibili a querela della persona offesa.
4. Tuttavia si procede d'ufficio e la pena è della reclusione da quattro a dieci anni se il fatto è commesso:
1. in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615 -ter, terzo comma;
2. in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

I reati di cui al primo e secondo comma dell'articolo 617 quater c.p. - modificato dalla citata Legge n. 90/2024 - sono due reati completamente autonomi: mentre il primo comma si occupa della intercettazione di informazioni fra due sistemi autonomi, il secondo si occupa della loro divulgazione, intendendo punire anche chi divulga comunicazioni intercettate da altri.
Esempi di condotte sanzionate sono:

- la creazione di un programma capace di intercettare le comunicazioni di posta elettronica indirizzate ad amministratori e dipendenti;
- l'intercettazione fraudolenta della comunicazione relativa all'autorizzazione, per via telematica o proveniente da sistema centralizzato, all'uso di una carta di credito.

Art. 617 quinquies
Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Chiunque, fuori dai casi consentiti dalla legge, 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 ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni

Tale articolo è stato aggiunto dall'art. 3, della L. 8 aprile 1974, n. 98, relativa alla riservatezza e della libertà e segretezza delle comunicazioni, modificato dall'art. 19 della Legge n. 238/2021 e quindi dalla Legge n. 90 del 26/06/2024.
Anche in tale articolo il legislatore, con riferimento alle condotte indicate, ha inserito l'avverbio "*abusive*".

È un reato di pericolo e per questo, ai fini della sua consumazione, non è necessario che l'effetto (interruzione, impedimento, intercettazione con raccolta e memorizzazione dei dati) si concretizzi.[6]

Art. 629
Estorsione informatica

1. Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.
2. La pena è della reclusione da sette a venti anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628.
3. Chiunque, mediante le condotte di cui agli articoli 615 -ter , 617 -quater , 617 -sexies , 635 -bis , 635 -quater e 635 -quinquies ovvero con la minaccia di compierle,
costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità

Il delitto di estorsione è aggravato (reclusione **da sei a venti anni** e multa da euro 5.000 a euro 15.000) se commesso mediante le condotte di accesso abusivo (615-ter) o danneggiamento informatico (635-bis, ter, quater, quinquies). **Sanzione per l'Ente (Art. 24-bis, comma 4-bis):** Sanzione pecuniaria **da 300 a 800 quote** e applicazione delle sanzioni interdittive (es. divieto di contrattare con la PA) per una durata non inferiore a due anni."

L'articolo, introdotto dalla L. 90 del 26/06/2024, mira a punire severamente l'estorsione informatica come reato autonomo.

Art. 635 bis
Danneggiamento di informazioni, dati e programmi informatici

1. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni.
2. La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

L'articolo in commento - – anch'esso modificato dalla citata Legge n. 90/2024, con notevole inasprimento delle pene edittali e la previsione di aggravanti ad effetto speciale - ricalca quanto

[6] Vale la pena di evidenziare che, con la Legge n. 90/2024, è stato introdotto l'art. 623-quater del codice penale, il quale prevede diminuzioni di pena per i reati previsti e puniti dagli artt. 615-ter, 615-quater, 617-quater, 617-quinquies e 617 sexies del codice penale allorchè "*il fatto risulti di lieve entità*".

previsto dall'art. 635 c.p. in materia di danneggiamento costituendone una "specialità": esso viene integrato anche nel caso in cui i file e dati cancellati possano essere recuperati.
E' solo il caso di accennare alla problematica legata alla proprietà "altrui" di dati e programmi, alla luce delle diffuse pratiche collegate al Cloud ed al Leasing.
Non è richiesto il dolo specifico e sono sanzionati comportamenti ed omissioni sia di chi agisce volendo esplicitamente e ricercando il danneggiamento che quella di chi è consapevole che il suo comportamento potrebbe comportare un danneggiamento ma confida nella sorte.
Esempio di una condotta riconducibile all'articolo in esame è la cancellazione, da parte di un dipendente, di dati dall'hard disk del personal computer della sua postazione di lavoro.

Art. 635 ter
Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico

1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.
2. La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione
o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.
La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3.

Questo articolo è stato inserito dalla Legge n. 48/2008 e, come l'art. 635 bis c.p., è stato oggetto di modifica da parte del D.Lgs. n. 7/2016 e da ultimo dalla Legge n. 90/2024 (anche qui con inasprimento delle pene e la previsione di aggravanti ad effetto speciale): esso costituisce un'ipotesi autonoma di reato e non, quindi, un'ipotesi aggravata dell'art. 635 bis c.p..
Si tratta delitto di pericolo, per cui la condotta perseguita deve essere diretta ed idonea a causare il danneggiamento informatico: si richiede, quindi, una valutazione esterna all'agente, sulla base della considerazione di condizioni storiche e sociali presenti al momento del fatto.

Art. 635 quater
Danneggiamento di sistemi informatici o telematici

1. *Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili*

sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni.

2. *Qualora dal fatto derivi la distruzione o il danneggiamento di sistemi di pubblica utilità, la pena è della reclusione **da tre a dieci anni**."*

Anche questo articolo è stato inserito dalla Legge n. 48/2008 e, come gli artt. 635 bis e 635 ter, è stato oggetto di modifica dapprima con il D.Lgs. n. 7/2016 e poi con la Legge n. 90/2024 (che ha aggravato le pene edittali e previsto aggravanti ad effetto speciale).

Rispetto all'articolato di cui all'art. 635 bis c.p., qui sono indicate ulteriori condotte criminose che portano al danneggiare od ostacolare il funzionamento del sistema informatico o telematico, non solo mediante distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui (art. 635 bis) ma anche "*attraverso l'introduzione o la trasmissione di dati, informazioni o programmi*".

Art. 635 quater.1
Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

1. Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, 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 è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.
2. La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 - ter , secondo comma, numero 1).
3. La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615 -ter , terzo comma».

Questo articolo è stato inserito dalla Legge n. 90 del 26/06/2024, che ha anche abrogato l'art. 615 quinquies c.p.: la fattispecie è volta a reprimere la diffusione di "*apparecchiature, dispositivi o programmi informatici*" diretti a danneggiare o interrompere un sistema "*informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti*". Si tratta, in altri termini, della diffusione di tutti i programmi rientranti nella categoria dei malware ma anche della diffusione di componenti hardware (smart card, pen drive, USB, ecc.) in grado di danneggiare sistemi informatici e/o telematici.

Nell'articolo in parola sono previste due distinte ipotesi di reato. Infatti, è punito chi diffonde, comunica o consegna un programma informatico (sia frutto del proprio ingegno, che di altri):

- volto o atto a danneggiare illecitamente un sistema informatico/telematico, le informazioni ed i programmi ad esso pertinenti;
- volto ad interrompere o alterare, seppur temporaneamente, il funzionamento di un sistema informatico/telematico.

Quindi, poco importa che il fine ultimo sia quello di procurare un danno od un'interruzione parziale perché si possa configurare il reato. Quest'ultimo è di tipo comune e si consuma nel momento in cui vengono messe in atto le condotte di diffusione, comunicazione o consegna: la semplice realizzazione di un virus informatico, quindi, di per sé non ha rilevanza penale alcuna, mentre la sua detenzione potrebbe essere sanzionata. L'elemento soggettivo richiesto è il dolo specifico.

Art. 635 quinquies
Danneggiamento di sistemi
informatici o telematici di pubblico interesse

1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 -bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.
2. La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.
La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)».

Questo articolo era stato originariamente inserito dalla Legge n. 48/2008 ed è stato integralmente sostituito dalla Legge n. 90/2024.
Esso costituisce un'ipotesi autonoma di reato e non un'ipotesi aggravata di quanto previsto dall'art. 635 quater c.p., è un reato di pericolo eppertanto l'integrazione della fattispecie non richiede che si produca il danneggiamento dei sistemi informatici e telematici di pubblica utilità, ovvero che ne sia effettivamente ostacolato il funzionamento[7].

2.1.2 Falsità e frode informatica ed illeciti negli approvvigionamenti di beni e servizi.

Mentre gli articoli indicati nei primi due commi dell'art. 24 *bis* del D.Lgs. n. 231/2001 hanno per "oggetto del reato" i sistemi informatici e telematici, il terzo comma si riferisce ai sistemi come "strumento" per poter commettere un reato, occupandosi della falsità di un "*documento informatico*" e di chi "*falsifica dati e programmi*" per commettere una frode.
Va notato che art. 24 del D.Lgs. n. 231/2001 (per quanto qui di interesse in relazione alla presente Parte Speciale), al primo comma richiama anche:

- gli incanti pubblici (art. 353 c.p.)
- la turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.);
- la frode nelle pubbliche forniture (art. 356 c.p.);
- il reato di frode informatica (art. 640-ter c.p.).

[7] con la Legge n. 90/2024, è stato introdotto l'art. 639-ter del codice penale, il quale prevede diminuzioni di pena per i reati previsti e puniti dagli artt. 629 terzo comma, 635-ter, 635-quater.1, e 635-quinquies del codice penale allorchè "*il fatto risulti di lieve entità*".

Tali reati presupposto, organicamente, verranno presentati in questa Parte Speciale, anche in virtù del nuovo Codice degli Appalti di cui al D.Lgs. n. 36/2023, che prevede la creazione di una sorta di ecosistema digitale, quale strumento per la digitalizzazione del ciclo di vita dei contratti e la piena effettività dell'*eProcurement*[8] (*cfr*. in particolare art. 22 del D.Lgs. n. 36/2023).

Art. 491 bis
Documenti informatici

1. Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.

L'art. 491-bis c.p. si riferisce specificatamente al "*documento informatico*", la cui definizione è contenuta alla lettera p) del comma 1 dell'art. 1 del D.Lgs. n. 82/ 2005 altrimenti noto come Codice dell'Amministrazione Digitale (CAD). Con la locuzione "*documento informatico"* ci si riferisce al *"documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".* La gestione del documento informatico è normata dal D.P.C.M. 13 novembre 2014 - *"Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".*
Il documento informatico per essere ritenuto tale deve essere sottoscritto con firma elettronica potendo, in caso contrario, soddisfare al più il requisito legale della forma scritta.
Il testo dell'articolo limita, infatti, l'ambito di applicazione ai documenti informatici aventi efficacia probatoria. Rispetto a quest'ultima, il principio generale, espresso nel **comma 1-bis) dell'art. 20 del CAD**, recita:

1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi é apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, é formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.

La figura che segue, riassume il valore probatorio per diversa tipologia di firma elettronica.

[8] Tale termine identifica un processo di approvvigionamento elettronico per il cui tramite vengono acquistati prodotti e servizi. La trasformazione digitale della Pubblica Amministrazione, così come prevede il Piano triennale per l'informatica nella PA, si basa sulla semplificazione e sull'innovazione dei processi, con l'obiettivo di migliorare l'efficienza e la qualità dei servizi al cittadino e alle imprese.

Figura 1 – Varie tipologie di firma

Mentre l'art. 491 bis c.p. si riferisce ad un documento e tutela la fede pubblica indipendentemente dall'utilizzo che ne viene fatto, il comma 1 dell'articolo 24 e il comma 3 dell'art. 24 bis del D.Lgs n. 231/2001, si riferiscono specificatamente alla frode informatica.
Recitano, infatti, gli artt. 640-ter e 640-quinquies c.p.:

Art. 640 ter
Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema .
La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61,

primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età.

Esempi di condotte riconducibili all'articolo in commento sono le seguenti:

- il dipendente che, utilizzando la "password" in dotazione, manomette la posizione debitoria, effettuando sgravi non dovuti e non giustificati;
- chiunque, dopo essersi appropriato della "password", responsabile di zona di una compagnia assicurativa, manipola i dati del sistema predisponendo false attestazioni per risarcimento dei danni.

Il secondo comma, nella parte in cui prevede *"ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema"* verrà trattato successivamente, in relazione all'art. 25 octies.1 del D.lgs. n. 231/01.

Art. 640 quinquies
Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

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

La norma è posta a presidio di un settore che sta assumendo grande rilevanza nel traffico giuridico nell'ambito delle firme elettroniche o sottoscrizioni digitali, le quali - a seconda di requisiti e caratteristiche - la legge equipara, a seconda dei casi, alla scrittura privata ovvero alla scrittura privata con sottoscrizione autenticata.
Concretamente la fattispecie potrebbe delinearsi nell'ipotesi in cui un Ente certificatore rilasciasse – ad esempio a fronte di una cospicua dazione in denaro – certificati di firma intestati a persone diverse dagli effettivi utilizzatori.

***

Per quanto attiene l'ambito **relativo alle pubbliche forniture**, i reati presupposto sono di seguito riportati.

Art. 353.
Turbata libertà degli incanti

Chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche Amministrazioni, ovvero ne allontana gli offerenti, è punito con la reclusione da sei mesi a cinque anni e con la multa da lire mille a diecimila.
Se il colpevole è persona preposta dalla legge o dall'Autorità agli incanti o alle licitazioni suddette, la reclusione è da uno a cinque anni e la multa da lire cinquemila a ventimila.
Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati, dirette da un pubblico ufficiale o da persona legalmente autorizzata; ma sono ridotte alla metà.

Art. 353-bis.

Turbata libertà del procedimento di scelta del contraente

Salvo che il fatto costituisca più grave reato, chiunque con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.

Art. 356.
Frode nelle pubbliche forniture

Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a lire diecimila.
La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente.

Va sottolineato che l'inserimento di questi reati nell'ambito della presente Parte Speciale viene esaminato solo per ciò che attiene la parte informatica, stante la digitalizzazione del ciclo di vita dei contratti operata con la Parte II del LIBRO I del D.Lgs. n. 36/2023.
Come anticipato, obbiettivo del legislatore è quello di digitalizzare l'intera procedura dei contratti pubblici, basandola sull'acquisizione di dati e sulla creazione di documenti nativi digitali, tramite piattaforme digitali in modo tale da rendere possibile l'interazione con le banche dati esistenti e consentendo così un arricchimento delle stesse con nuovi dati prodotti dalle singole procedure.
In particolare, l'art. 22 del D.Lgs. n. 36/2023, rubricato *"ecosistema nazionale di approvvigionamento digitale (e-procurement)"*, prevede che:
"*L'ecosistema nazionale di approvvigionamento digitale (e-procurement) è costituito dalle piattaforme e dai servizi digitali infrastrutturali abilitanti la gestione del ciclo di vita dei contratti pubblici, di cui all'articolo 23 e dalle piattaforme di approvvigionamento digitale utilizzate dalle stazioni appaltanti di cui all'articolo 25.*
2. Le piattaforme e i servizi digitali di cui al comma 1 consentono, in particolare:
a) la redazione o l'acquisizione degli atti in formato nativo digitale;
b) la pubblicazione e la trasmissione dei dati e documenti alla Banca dati nazionale dei contratti pubblici;
c) l'accesso elettronico alla documentazione di gara;
d) la presentazione del documento di gara unico europeo in formato digitale e l'interoperabilità con il fascicolo virtuale dell'operatore economico;
e) la presentazione delle offerte
f) l'apertura, la gestione e la conservazione del fascicolo di gara in modalità digitale;
g) il controllo tecnico, contabile e amministrativo dei contratti anche in fase di esecuzione e la gestione delle garanzie.
3. Le basi di dati di interesse nazionale alimentano l'ecosistema nazionale di approvvigionamento digitale, ai sensi dell'articolo 60 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82".

Il sistema nazionale di approvvigionamento digitale – in estrema sintesi - è composto da piattaforme informatiche e servizi materiali digitali che facilitano lo scambio di dati e di informazioni su tali piattaforme, consentendo la gestione completa del ciclo di vita dei contratti pubblici. La piattaforma digitale deve essere interconnessa e interoperabile con la *"Banca Dati Nazionale dei Contratti*

Pubblici" (anche solo "*BDNCP*")[9]. A tal fine, essa deve possedere specifici requisiti tecnici e operare secondo regole comuni che sono state stabilite dalla Agenzia per l'Italia Digitale (anche solo "*AGID*")[10] con la determinazione n. 137 del 01.06.2023 (fermo che le modalità procedurali e operative per richiedere la certificazione della piattaforma sono, allo stato, contenute nella determina AGID n. 218 del 25.09.2023).
L'art. 21 del D.Lgs. n. 36/2023, rubricato "*ciclo di vita digitale dei contratti pubblici*", consente di individuare **le fasi del ciclo di vita dei contratti** che, più in dettaglio, risultano essere quelle presentate in figura seguente.

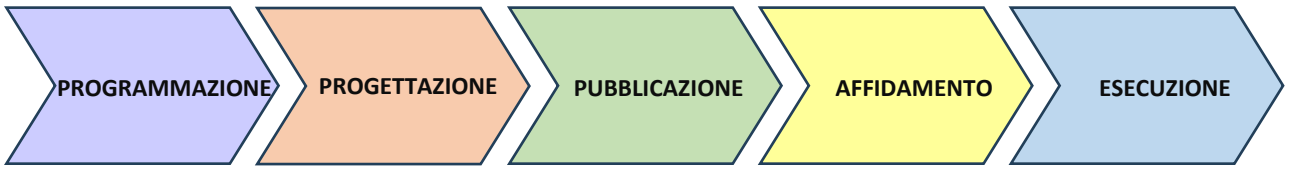

Figura 2 – Fasi del ciclo di vita dei contratti

Per meglio comprendere i contenuti di ogni fase del processo, si richiama la delibera ANAC n. 261/2023[11] che riporta, all'articolo 10 di seguito trascritto, le informazioni che ciascuna stazione appaltante deve trasmettere per ogni fase, individuando così le attività riconducibili a ciascuna fase.

Articolo 10
Informazioni che le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere alla BDNCP

10.1 Le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere tempestivamente alla BDNCP, per il tramite delle piattaforme di approvvigionamento certificate, le informazioni riguardanti:

*a) **programmazione***
1. *il programma triennale ed elenchi annuali dei lavori;*
2. *il programma triennale degli acquisti di servizi e forniture*

*b) **progettazione e pubblicazione***
1. *gli avvisi di pre-informazione*
2. *bandi e gli avvisi di gara*
3. *avvisi relativi alla costituzione di elenchi di operatori economici*

*c) **affidamento***
2. *gli avvisi di aggiudicazione ovvero i dati di aggiudicazione per gli affidamenti non soggetti a pubblicità*

[9] https://dati.anticorruzione.it/superset/dashboard/appalti/?native_filters_key=nQ8n_sMV8P_8oK28njCN2dNf8WgK59ESKI5ns-Gw8kTNJkJeEH5hjWBATUjxpyU_

[10] https://www.agid.gov.it/

[11] Senza pretesa di esaustività: quanto agli obblighi di pubblicazione si veda l'art. 27 del D.lgs. n. 36/2023 e la delibera ANAC n. 263/2023 del 20 giugno 2023; quanto agli obblighi di trasparenza si veda l'art .28 del D.lgs.36/2023 e la delibera ANAC n. 264/2023, come modificata con delibera ANAC n. 601 del 19 dicembre 2023.

3. *gli affidamenti diretti*

d) ***esecuzione***

1. *La stipula e l'avvio del contratto*
2. *gli stati di avanzamento*
3. *i subappalti*
4. *le modifiche contrattuali e le proroghe*
5. *le sospensioni dell'esecuzione*
6. *gli accordi bonari*
7. *le istanze di recesso*
8. *la conclusione del contratto*
9. *il collaudo finale*

e) ogni altra informazione che dovesse rendersi utile per l'assolvimento dei compiti assegnati all'ANAC dal codice e da successive modifiche e integrazioni.

In tale contesto - posto che ciascuna Stazione Appaltante diventa così parte dell'ecosistema digitale nella gestione dei contratti - l'Ente ha l'obbligo, sancito dall'art. 19 comma 1 del D.Lgs. n. 36/2023[12], anche "*di protezione dei dati personali e di sicurezza informatica*".

In generale, quindi, tutte le problematiche legate ad un malfunzionamento o ad una compromissione della sicurezza possono creare un pregiudizio per il funzionamento del sistema di *eProcurement*, così come la mancata gestione dei file di log possono portare a comportamenti fraudolenti o disattenti da patre di coloro che sono abilitati ad accedere al sistema.

L'elemento umano rappresenta, infatti, uno dei problemi più rilevanti e per il quale, risultano necessari la predisposizione di percorsi di sensibilizzazione e training, nonché di meccanismi di controlli a campione sui log delle attività e su specifici contratti a Campione anche in sinergia con il Responsabile della prevenzione della corruzione e della trasparenza (RPCT), volti a minimizzare comportamenti opportunistici.

L'art. 19, comma 2 del D.Lgs. n. 36/2023 prescrive, poi, che tutte le attività inerenti al ciclo di vita dei contratti pubblici debbano essere gestite *"…nel rispetto delle disposizioni del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82…"*.

Da ultimo merita porre l'attenzione sull'art. 30 del D.Lgs. n. 36/2023 (rubricato *"Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici"*), per il quale la selezione della controparte potrebbe essere figlia di un processo legato all'intelligenza artificiale. Infatti, il primo comma sancisce che "*per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia*".

Se la blockchain non crea problemi di utilizzo, l'uso dell'intelligenza artificiale potrebbe essere, in realtà, un escamotage per coprire assegnazioni pilotate, posto che, nonostante le previsioni legislative, una piena giustificabilità delle scelte risulta impossibile e che gli algoritmi alla base delle procedure automatiche potrebbero essere stati "allenati" in maniera impropria o fraudolenta.

È solo il caso di citare che è stato appena adottato dalla Commissione Europea (ed attende solo la pubblicazione) l'**Artificial Intelligence Act**[13], che regolerà le modalità di utilizzo dell'intelligenza artificiale anche nelle applicazioni alla vita reale.

[12] "*Le stazioni appaltanti e gli enti concedenti assicurano la digitalizzazione del ciclo di vita dei contratti nel rispetto dei principi e delle disposizioni del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, garantiscono l'esercizio dei diritti di cittadinanza digitale e operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica".*

[13] L'adozione è del 26 gennaio 2023.

2.2 Delitti contro la personalità individuale

Un altro ambito di applicazione del D.Lgs. n. 231/2001 che può ingenerare responsabilità dell'Ente e che ha un conseguenze di un certo rilievo, anche dal punto di vista reputazionale, è quello che vede negli strumenti informatici utilizzati un possibile strumento per la commissione dei reati ricompresi nel novero dei delitti contro la personalità individuale.
In particolare, il comma 1, lett. b) e il comma 1, lett. c), dell'art. **25 quinquies** del D.Lgs. n. 231/01, rimandano alla prostituzione ed alla pornografia minorile.
Si riportano, di seguito, gli articoli del codice penale – qui di interesse - richiamati dall'art. 25 quinquies.

Art. 600 bis
Prostituzione minorile.

1. È punito con la reclusione da sei a dodici anni e con la multa da euro 15.000 a euro 150.000 chiunque:
1) recluta o induce alla prostituzione una persona di età inferiore agli anni diciotto;
2) favorisce, sfrutta, gestisce, organizza o controlla la prostituzione di una persona di età inferiore agli anni diciotto, ovvero altrimenti ne trae profitto.
2. Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi, è punito con la reclusione da uno a sei anni e con la multa da euro 1.500 a euro 6.000.

In Giurisprudenza l'orientamento prevalente è quello di considerare un'accezione ampia di prostituzione, come "*qualsiasi prestazione sessuale effettuata dietro corrispettivo, senza che la prestazione sessuale debba necessariamente consistere nella «congiunzione carnale»*": infatti, qualsiasi attività diretta a eccitare e soddisfare la libidine sessuale del destinatario si configura come "*prestazione sessuale» e integra prostituzione se è appositamente retribuita dal destinatario della medesima*".
Si ha prostituzione, quindi, se sussistono:

- un generico atto dispositivo del proprio corpo (anche la voce) a sfondo sessuale da parte di chi si prostituisce;
- l'obiettivo del raggiungimento della soddisfazione sessuale da parte del destinatario dell'atto;
- l'interazione fra la condotta prostitutoria ed il risultato della stessa;
- il pagamento di un corrispettivo per l'azione.

Proprio in relazione a questo concetto di prostituzione, gli strumenti informatici costituiscono uno dei possibili canali per il concretizzarsi del reato.

Art. 600 ter
Pornografia minorile.

1. È punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 chiunque:
1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;
2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto.

2. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.
3. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.
4. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.
5. Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.
6. Salvo che il fatto costituisca più grave reato, chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto è punito con la reclusione fino a tre anni e con la multa da euro 1.500 a euro 6.000.
7. Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

L'elemento centrale di tutela di cui all'art. 600 ter c.p. è il minore, ponendo l'accento non tanto sulla protezione del fruitore (come accade, invece, nelle norme in materia di osceno), ma sulla protezione del protagonista stesso dell'esibizione o della riproduzione pornografica.
Il concetto di pornografia minorile è molto ampio e ben chiarito dal comma 7 che fa rientrare in questo ambito "*ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali*".

Il reato di pornografia minorile commesso per via telematica ha natura istantanea ed è integrato dall'immissione in rete del materiale pedopornografico. Infatti, la divulgazione di materiale pornografico implica la volontà consapevole di divulgarlo e o diffonderlo.

Art. 600 quater
Detenzione di materiale pornografico.

1. Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.
2. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

Nel reato in commento, ad essere punito è chi rappresenta il "consumatore finale", punito non per aver cercato di far circolare materiale pornografico che coinvolge minori ma per la semplice detenzione (è non più chi produce materiale pornografico con minori o procede allo sfruttamento sessuale del minore).
La detenzione deve essere consapevole e non limitarsi a singoli frammenti di file, non coordinati e sequenziali come, ad esempio, materiale "scaricato" in internet, e non costituito in files completi, incorrotti e visionabili o comunque potenzialmente fruibili per mezzo degli ordinari strumenti e competenze informatiche, dei quali sia provata la disponibilità in capo all'utente.

Pur tuttavia, il reato sussiste anche se l'agente procede alla cancellazione di file pornografici con minori "scaricati" da internet, mediante l'allocazione nel "cestino" del sistema operativo del personal computer, in quanto facilmente recuperabili.
Il reato di detenzione di materiale pornografico con minori è configurabile anche nel caso in cui il materiale sia stato prodotto con il consenso del minore stesso.

Anche se non esplicitamente richiamato, l'art. 600 quater.1 c.p. introdotto dall'art. 4 della L. 6 febbraio 2006, n. 38, è di fondamentale importanza per comprendere quali azioni possano configurare un reato ricompreso negli artt. 600 ter e 600 quater c.p..

Art. 600 quater.1
Pornografia virtuale.

1. Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.
2. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Tale articolo è stato inserito dall'art. 4 della Legge n. 38/2006.
Un esempio di comportamento sanzionato è stato quello di chi deteneva una pluralità di immagini e video di carattere pedopornografico virtuale (ottenuti, del resto, mediante file sharing) che si sostanziavano in scene stilizzate e disegnate come cartoni animati ma elaborate a tal punto da apparire vere, anche se non reali.

art. 609-undecies c.p.
Adescamento di minorenni

Il reato di adescamento di minorenni sanziona chiunque, allo scopo di commettere reati di natura sessuale o pedopornografica, instaura un contatto con un minore di anni diciotto attraverso qualsiasi modalità (inclusi gli strumenti informatici e telematici).
In linea con quanto previsto dall'Art. 600-quater.1 c.p. (Pornografia virtuale), la Società presta particolare attenzione alle condotte che coinvolgono materiale pedopornografico realizzato mediante tecniche di elaborazione grafica. Tali immagini, sebbene non associate a situazioni reali, sono elaborate a tal punto da far apparire come vere scene non reali (es. immagini stilizzate o "cartoni animati" iper-realistici).
Esempi di comportamenti sanzionati A titolo esemplificativo, ma non esaustivo, rientrano tra le condotte vietate:

- L'adescamento di un minore finalizzato alla produzione o alla richiesta di invio di immagini pornografiche, anche qualora tali immagini vengano successivamente rielaborate o "virtualizzate".
- L'utilizzo di sistemi informatici aziendali per la detenzione o la condivisione (tramite file sharing o altri canali) di video o immagini di carattere pedopornografico virtuale, anche sotto forma di disegni o animazioni digitali, la cui qualità rappresentativa simuli situazioni reali coinvolgenti minori.

Principi di comportamento e prevenzione Ai fini del Modello 231, è fatto divieto assoluto a tutti i destinatari di:

1. Utilizzare gli strumenti informatici aziendali (PC, smartphone, connessione internet) per accedere, scaricare o diffondere materiale che possa integrare la fattispecie di pornografia virtuale, indipendentemente dalla consapevolezza della "non realtà" fisica del soggetto rappresentato.
2. Adottare condotte comunicative online che possano essere interpretate come tentativi di adescamento o manipolazione di soggetti minorenni, anche qualora l'interazione avvenga tramite canali social o piattaforme di messaggistica per scopi apparentemente estranei all'attività lavorativa ma utilizzando asset aziendali.

Va, infine, riportato l'art. 603-bis c.p..

Art. 603-bis.
Intermediazione illecita e sfruttamento del lavoro

Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:
1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.
Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.
Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:
la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.
Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà:
1) il fatto che il numero di lavoratori reclutati sia superiore a tre;
2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;
3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

2.3 Delitti in materia di strumenti di pagamento diversi dai contanti

Il continuo processo di dematerializzazione dei pagamenti ha imposto al legislatore la previsione di strumenti di repressione idonei a salvaguardare la sicurezza degli scambi economici e tutelare i consociati da frodi sempre più sofisticate.
In tal senso, in data 29.11.2021 è stato pubblicato in Gazzetta Ufficiale il D.Lgs n. 184/2021 recante "*Attuazione della direttiva UE 2019/713 del Parlamento Europeo e del Consiglio, del 17 aprile 2019,*

relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio".
Tale Decreto Legislativo, entrato in vigore in data 14.12.2021, ha introdotto l'art. **25-ocities.1** nel D.Lgs. n. 231/2001 rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*", estendendo, di fatto, la responsabilità amministrativa degli enti ai reati di cui agli artt. 493 ter c.p., 493 quater c.p. e 640 ter c.p. (nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale).
L'art. 1 del D.Lgs. 184/2021 ha introdotto definizioni nuove anche per il Codice Penale, le quali devono essere tenute in considerazione ai fini dell'interpretazione delle fattispecie:
<<Agli effetti della legge penale si intende per:
a) «strumento di pagamento diverso dai contanti» un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali;
b) «dispositivo, oggetto o record protetto» un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma;
c) «mezzo di scambio digitale» qualsiasi moneta elettronica definita all'articolo 1, comma 2, lettera h-ter, del decreto legislativo 1° settembre 1993, n. 385, e la valuta virtuale;
d) «valuta virtuale» una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente>>.
La nozione di "valuta virtuale" include ora anche i nuovi asset digitali definiti dal Regolamento MiCAR (UE 2023/1114).

In sintesi, i citati reati presupposto intendono reprimere i comportamenti legati:

- all'utilizzo di uno strumento di pagamento diverso dal denaro contante di cui il soggetto non è titolare;
- alla falsificazione degli strumenti di pagamento diversi dal denaro contante;
- al possesso, cessione o acquisizione di strumenti di pagamento di provenienza illecita, falsificati o alterati;
- alla produzione, importazione, esportazione, vendita, trasporto, distribuzione, messa a disposizione o in qualsiasi modo procurata - a sé o a altri – disponibilità di apparecchiature, dispositivi o programmi informatici che permettono la commissione dei reati riguardanti strumenti di pagamento diversi dai contanti;
- al trasferimento di denaro, di valore monetario o di valuta virtuale mediante frode informatica.

Di seguito, si riportano i disposti normativi sopra richiamati e contenuti nell'art. 25 octies.1 del D.lgs. n. 231/01:

Art. 493-ter.
Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti
Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti è punito con la reclusione da uno a

cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.
In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.
Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.

La norma è stata inserita dall'art. 4, comma 1 lett. a), del D.Lgs n. 21/2018, oggetto di modifica dall'art. 2 del D.Lgs n. 84/2021, a decorrere dal 14 dicembre 2021 (il quale ha modificato anche la rubrica della fattispecie).
In tale articolo sono indicate tre distinte condotte criminose, punite in egual modo: chi si avvale, al fine di trarne profitto per sé o per altri, di uno strumento di pagamento diverso dal denaro contante di cui non è titolare (non è richiesto che venga sottratta la carta di credito ad altro soggetto, ma anche semplicemente avendola trovata), chi, sempre al fine di trarne profitto, falsifica tali strumenti di pagamento, ovvero possiede, cede o acquisisce i predetti strumenti di provenienza illecita, falsificati o alterati.
Il reato si consuma nel momento in cui vengono utilizzate le carte, falsificate o cedute a terzi. Non è quindi richiesta l'effettivo conseguimento di un profitto, purché venga accertato il dolo specifico.

Art. 493-quater.
Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

Salvo che il fatto costituisca più grave reato, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.
In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Questo articolo è stato inserito dall'art. 2, comma 1, lett. B), del D.lgs 184/2021, a decorrere dal 14 dicembre 2021.
Rispetto all'art. 493 ter c.p., tale fattispecie punisce chi, al fine di utilizzarle o permettere di utilizzare ad altri, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi

modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che permettono la commissione dei reati riguardanti strumenti di pagamento diversi dai contanti.

Art. 640-ter.
Frode informatica

[…] La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.
[…]

Il secondo comma dell'art. 640 ter c.p. è stato modificato dall'art. 2, comma 1, lett. c) del citato D.lgs n. 184/2021, a decorrere dal 14 dicembre 2021.
In tal senso il legislatore ha voluto punire il caso in cui la frode informatica produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

2.4 Delitti in materia di violazione del diritto di autore

Il tema della tutela del diritto d'autore è tra quelli che maggiormente hanno risentito (e risentono tuttora) della 'rivoluzione digitale' e, proprio per questo, su di esso si è concentrata l'attenzione del legislatore, come dimostrano i numerosi interventi normativi succedutisi negli ultimi anni.
Le moderne tecnologie informatiche - in primis il Web - hanno radicalmente mutato lo scenario in cui le norme giuridiche sono destinate ad essere applicate e ad esplicare i propri effetti: il tradizionale legame fra l'opera dell'ingegno ed il supporto materiale su cui si colloca, si affievolisce. Non esiste più, infatti, la necessità di avere un supporto su cui memorizzare un'opera dell'ingegno.
La rivoluzione informatica non ha, però, solo mutato il contesto di riferimento ma ha anche portato alla nascita di altre categorie di beni protetti da copyright: i beni informatici costituiti da programmi per elaboratore, banche di dati, opere multimediali che, per le loro peculiari caratteristiche, hanno richiesto l'introduzione di una disciplina di tutela ad hoc.
La disciplina normativa del diritto d'autore, pur enunciata nei suoi caratteri fondamentali nelle norme del codice civile, è sostanzialmente contenuta nella Legge 22 aprile 1941, n. 633, il cui testo originario è stato più volte oggetto di modifiche o di integrazioni da parte del nostro Legislatore. In verità quest'ultimo disposto normativo presenta, nel suo articolato, molte incongruenze e lascia spesso spazio ad interpretazioni, spesso non univoche in giurisprudenza, con eventuali sovrapposizioni o sperequazioni nell'applicazione delle sanzioni che censurano diversi comportamenti.
L'art. 1 della Legge n. 633/1941 definisce l'oggetto della disciplina stabilendo che: "*Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione. Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore".*

La Legge 23 luglio 2009, n. 99 – "*Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*" - ha modificato la disciplina del D.Lgs n. 231/2001, introducendo l'art.

25-novies, che fa rientrare tra i reati presupposto anche le seguenti fattispecie previste della Legge n. 633/1941:

- articolo 171, primo comma, lettera a-bis) e terzo comma;
- articolo 171 bis;
- articolo 171-ter;
- articolo 171-septies;
- articolo 171-octies.

In sintesi, i reati presupposto intendono reprimere e censurare comportamenti legati:

- all'immissione in rete di opere protette dal diritto d'autore (programmi per elaboratore, banche dati, opere audiovisive e musicali, libri, fotografie, …);
- alla diffusione di opere protette da diritto d'autore con deformazioni tali da comportare offesa all'onore ed alla dignità dell'autore;
- all'usurpazione della paternità di un'opera;
- alla diffusione o la commercializzazione per scopi economico-imprenditoriali di opere protette dal diritto d'autore;
- alla duplicazione per scopi non personali di film, musica, libri, spettacoli, banche dati;
- all'illegale decriptazione e trasmissione di segnali digitali o analogici di tipo televisivo;
- alla partecipazione nella filiera dell'immissione sul mercato di dispositivi e metodologie capaci di eludere, rimuovere, superare eventuali protezioni o capaci di decodificare segnali criptati.

Di seguito, si riportano i disposti normativi sopra richiamati.

Art. 171-bis

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

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

L'art. 171-bis - introdotto dal D.Lgs. n. 518/1992, che ha esteso la tutela del Diritto d'Autore ai programmi per elaboratore - è stato oggetto di modifiche da parte del D.Lgs. n. 169/1999, che ha ulteriormente ampliato l'ambito di tutela alle banche dati, e quindi dalla Legge n. 248/2000.
Il bene giuridico tutelato riguarda esclusivamente gli interessi patrimoniali dei titolari dei diritti di sfruttamento economico del software o delle banche dati, mentre l'elemento oggettivo è legato ad una pluralità di azioni messe in campo dall'agente, accomunate dall'effetto di ledere i legittimi diritti patrimoniali e da una condotta "*abusiva*", ovvero esercitata da chi non "*ne ha diritto*" .
L'elemento soggettivo che qualifica il reato è lo "*scopo commerciale o imprenditoriale*": in tale scopo rientrano non solo le condotte di chi intende successivamente "*cedere a titolo oneroso*" un software ma anche di chi, nell'ambito di una generica attività imprenditoriale, consegue un risparmio di spesa.
Esemplificando: mentre una duplicazione di software freeware o la creazione di copie di sicurezza non costituiscono un reato, quando un soggetto pone in essere condotte (distribuzione, vendita, locazione,…) senza che la licenza glielo consenta, commette un illecito rientrante in questo ambito.
E' il caso, ad esempio, di un software legittimamente acquistato che viene installato su più elaboratori (*over licencing*): questa pratica consente, infatti, di ottenere un maggior profitto per effetto di un risparmio di spesa.
Secondo la giurisprudenza la semplice detenzione di programmi per elaboratore privi delle relative licenze d'uso (senza che vi sia stato alcun ulteriore accertamento idoneo a provare sia l'origine illecita dei programmi che la consapevolezza della loro illiceità) non può ritenersi da sola condotta sufficiente ad integrare il delitto di cui all'art. 171 bis, comma 1, della Legge n. 633/1941 .
La seconda tipologia di reati sanzionata dall'art. 171-bis è legata alla rimozione o elusione funzionale di protezioni poste a tutela di un programma per elaboratore: il dolo specifico è legato al profitto (maggior ricavo o minore spesa) ed i comportamenti sono legati alla violazione del codice di ritorno (usato, ad esempio, da Microsoft), alla inertizzazione dei dongle. Nell'ambito di tutela, il secondo comma fa rientrare anche le banche dati.
Esempi di comportamenti integranti il reato sono: (i) la realizzazione di programmi ricavati dallo sviluppo o da modifiche del prodotto originale; (ii) l'utilizzo presso uno studio professionale di "software" illecitamente riprodotti.

Art. 171-ter

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da € 2.582 a € 15.493 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, 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;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, 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;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, 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 alle lettere a) e b);
d) 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;
e) 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;
f) 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.
f-bis) 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 di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;
h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, 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;
h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931 n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.
2. È punito con la reclusione da uno a quattro anni e con la multa da € 2.582 a € 15.493 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.
3. La pena è diminuita se il fatto è di particolare tenuità.
4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.
5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

L'art. 171-ter rappresenta uno degli articoli più importanti in relazione alla tutela del Diritto d'Autore e risulta frequentemente applicato.
Tale disposto, inserito dal D.Lgs. n. 685/1994 - e successivamente modificato, da ultimo con la Legge n. 93/2023 – è di fatto volto a tutelare: (i) le opere destinate al circuito televisivo e cinematografico; (ii) le altre opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali ovvero le opere multimediali.
Le condotte sanzionate sono descritte oggettivamente e, per la punibilità, è richiesta la finalità di lucro dell'agente: non rientra quindi nell'art. 171-ter la duplicazione di prodotti intellettuali per fini personali propri o di un soggetto terzo diverso dall'autore della duplicazione (quest'ultimo caso solo a patto che la cessione sia a titolo gratuito).
Va sottolineato che il reato ha nauta di pericolo e, quindi, la semplice rimozione delle protezioni o l'alterazione delle informazioni elettroniche relative ai diritti d'autore (ex art. 102-quinquies) integrano il reato, e ciò anche se non si verifica un successivo utilizzo illegale.
In giurisprudenza si afferma la mancanza di un rapporto di specialità fra le condotte di cui all'art. 171-ter della Legge n. 633/1941 e quelle dell'art. 648 del codice penale: con la conseguenza che, in caso di reato, possono essere applicate entrambe le sanzioni.
Esempi di condotte integranti la fattispecie di reato in commento sono: (i) dell'articolo in esame sono: (i) la diffusione in pubblico di opere dell'ingegno di qualsiasi genere in violazione sia delle norme che disciplinano il mezzo di diffusione (stazioni televisive o radiofoniche prive di concessioni) che di quelle disciplinano l'oggetto diffuso (mancata corresponsione degli oneri dovuti alla SIAE); (ii) la riproduzione abusiva di brani musicali in assenza di preventiva regolamentazione dei rapporti con i soggetti titolari dei diritti connessi; (iii) la riproduzione abusiva di opere protette dal diritto d'autore che non sia connotata dal carattere di mera occasionalità; (iv) la riproduzione di singole opere o brani di opere dell'ingegno effettuata mediante fotocopie che superano il limite del quindici per cento di ogni volume, ovvero in assenza del compenso forfettario a favore degli aventi diritto o per uso non personale; (v) la detenzione a scopo commerciale di programmi per elaboratore abusivamente riprodotti, anche se finalizzata ad un uso esclusivamente dimostrativo o promozionale di detti programmi.

Art. 171-septies.

1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:
a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

L'articolo è stato introdotto dall'art. 17 della Legge n. 240/2000 per anticipare, in via prodromica, i legittimi interessi connessi allo sfruttamento dell'opera dell'ingegno.

Art. 171-octies.

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da € 2.582 a € 25.822 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.
2. La pena non è inferiore a due anni di reclusione e la multa a € 15.493 se il fatto è di rilevante gravità.

L'articolo è stato inserito dalla Legge n. 248/2000 per tutelare le trasmissioni audiovisive e successivamente modificato dalla Legge n. 373/2000, che ha operato una depenalizzazione delle sole attività di commercializzazione dei suddetti dispositivi.
Rimane sanzionata la condotta di chi utilizza, a fini fraudolenti e per uso pubblico, apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite e via cavo, in forma sia analogica sia digitale. Secondo alcuni vi sarebbe una sovrapposizione con le previsioni dell'art. 171-ter lett f) (vedasi il caso di chi, a pagamento, installa un decoder per l'accesso ad un segnale criptato non a pagamento).

Art. 171.

1. Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da 51 € a 2.065 € chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
[…]
a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
[…]
3. La pena è della reclusione fino ad un anno o della multa non inferiore a € 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Stante il fiorire di articoli aspecifici, all'art. 171 sembra riservato il compito di colmare un eventuale vuoto residuale, In realtà è l'unico articolo che si occupa della tutela dei diritti del creatore dell'opera intellettuale, a differenza di quanto avviene, invece, con gli altri articoli della Legge n. 633/1941.
Esso trova applicazione con riferimento ai diritti diversi dagli interessi patrimoniali (ad esempio si applica a chi, prima della pubblicazione e diffusione dell'opera, vende a terzi una copia pirata di un supporto che contiene l'opera stessa; oppure in caso di noleggio a fine di lucro di supporti (come, ad esempio, un DVD) sui quali sono registrate delle opere protette da diritto d'autore.

2.5 Delitti contro la Dignità e Personalità Individuale

Il reato di **Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.)** è un delitto contro la personalità individuale inserito nel catalogo dei reati presupposto del D.Lgs. 231/01 dall'**Art. 25-terdecies**.

I reato punisce diverse condotte legate all'odio discriminatorio:

- Propaganda: Diffusione di idee fondate sulla superiorità o sull'odio razziale o etnico.

- Istigazione: Incitamento a commettere atti di discriminazione o atti di violenza per motivi razziali, etnici, nazionali o religiosi.
- Associazionismo: Partecipazione o assistenza ad organizzazioni che hanno tra i propri scopi l'incitamento alla discriminazione o alla violenza.
- Negazionismo (Aggravante): La pena è aumentata se la propaganda o l'istigazione si fondano sulla negazione, minimizzazione grave o apologia della Shoah, dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

3 SANZIONI.

L'art. 10 del D.Lgs. n. 231/2001 dispone che: "1. Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria. 2. La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento né superiore a mille. 3. L'importo di una quota va da un minimo di euro 258 a un massimo di euro 1.549. 4. Non è ammesso il pagamento in misura ridotta".
L'art. 11 del medesimo Decreto precisa i criteri di commisurazione della sanzione pecuniaria stabilendo che "1. Nella commisurazione della sanzione pecuniaria il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. 2. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione. 3. Nei casi previsti dall'articolo 12, comma 1, l'importo della quota è sempre di euro 103."

L'articolo 24 bis, l'art. 24 e l'art. 25 quinquies del D.Lgs. n. 231/2001, prevedono sia sanzioni pecuniarie che accessorie (interdittive) applicabili all'Ente in caso di commissione di reati ivi previsti. La tabella che segue riassume i profili sanzionatori.

24 bis c.1 (da 200 a 700 quote)	**Art. C.P.**
Accesso abusivo ad un sistema informatico o telematico.	615 ter
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	617-quater
Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	617-quinquies
Danneggiamento di informazioni, dati e programmi informatici	635-bis
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	635-ter
Danneggiamento di sistemi informatici o telematici	635-quater
Danneggiamento di sistemi informatici o telematici di pubblica utilità	635-quinquies
24 bis c.1 bis (da 300 a 800 quote)	**Art. C.P.**

Estorsione	629 c.3
24 bis c.2 (sino a 400 quote)	**Art. C.P.**
Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici	615 quater
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informativo o telematico	635-quater.1
24 bis c.3 (sino a 400 quote)	**Art. C.P.**
Falsità di documenti informatici.	491 bis
Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	640-quinquies
24 c.1 (fino a 500 quote; da 200 a 600 se profitto rilevante)	**Art. C.P.**
Frode informatica (in danno dello Stato o di altro Ente pubblico)	640 ter
Turbata libertà degli incanti	353
Turbata libertà del procedimento di scelta del contraente	353-bis
Frode nelle pubbliche forniture	356
25 quinquies c.1 lett. b (da 300 a 800 quote)	**Art. C.P.**
Induzione, favoreggiamento o sfruttamento della prostituzione minorile	600 bis c.1
Realizzazione di esibizioni pornografiche con minori; produzione di materiale pornografico con minori; induzione alla partecipazione di minori ad esibizioni pornografiche.	600 ter c.1
Commercio di materiale pornografico cui partecipano minori.	600 ter c.2
25 quinquies c.1 lett. c (da 200 a 700 quote)	**Art. C.P.**
Compimento di atti sessuali con un minore	600 bis c.2
Distribuzione, divulgazione, diffusione e pubblicizzazione anche per via telematica, di materiale pornografico con minori; Divulgazione di notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori	600 ter c.3 609-undecies
Offerta e/o cessione di materiale pornografico cui partecipano minori.	600 ter c.4
Acquisizione e detenzione di materiale pornografico realizzato utilizzando minori	600 quater

Analogamente la tabella che segue rispetto ai reati presupposto previsti dalla Legge n. 633/41.

25 octies.1 c.1 lett. A e c. 2 lett. B (da 300 a 800 quote)	**Art C.P.**
Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti	493-ter

Altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal C.P., quando ha ad oggetto strumenti di pagamento diversi dai contati, se la pena della reclusione non è inferiore a 10 anni	
25 octies.1 c.1 lett. B e c.2 lett. A (sino a 500 quote)	**Art. C.P.**
Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti	493-ter
Frode informatica (nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale)	640-ter
Altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal C.P., quando ha ad oggetto strumenti di pagamento diversi dai contati, se la pena della reclusione è inferiore a 10 anni	
25 novies (fino a 500 quote)	**art L.633**
Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa.	171 c.1 lett. a-bis)
Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione.	171 c.3
Importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di Software. Azioni atte a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di Software. Violazione diritto d'autore in relazione a banche dati.	171 bis
Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico di opere dell'ingegno e banche dati;	171 ter
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione.	171 septies
Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.	171 octies

25 terdecies	
Propaganda e istigazione alla discriminazione	(604-bis c.p.)

Le **sanzioni interdittive** che possono accompagnarsi alla sanzione pecuniaria in ipotesi di integrazione dei citati illeciti sono esclusivamente quelle previste alle lettere c), d) ed e) dall'articolo 9, comma 2, del D.Lgs. n. 231/2001 e s.m.i. di seguito riportato:

D.Lgs. 231/01 e s.m.i.
Art. 9. Sanzioni amministrative

... omissis...
Le sanzioni interdittive sono:
a) l'interdizione dall'esercizio dell'attività;
b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) il divieto di pubblicizzare beni o servizi.

La tabella che segue, infine, riassume le sanzioni pecuniarie ed interdittive in relazione ai reati trattati in questa Parte Speciale.

		SANZIONE / Fonte	art. 24	24 bis				25 quinquies c.1		25 novies	25-terdecies
			c.1	c.1	c.1.bis	c.2	c.3	lett . b	lett. c	c.1	
Art. 9 c.1		**pecuniaria**	0-500 (200-600)	200-700	300-800	0-400	0-400	300-800	200-700	0-500	Da 200 a 800 quote
		interdittive									
	Art. 9 c.2	a) interdizione		X	X (>2 anni)			X (>1 anno)		X (<1 anno)	X (>1 anno)
	Art. 9 c.2	b) sospensione o revoca autorizzazioni licenze		X	X (>2 anni)	X		X (>1 anno)		X (<1 anno)	X (>1 anno)
	Art. 9 c.2	c) divieto di contrattare con la P.A.	X		X (>2 anni)		X	X (>1 anno)		X (<1 anno)	X (>1 anno)

		d) esclusione o revoca agevolaz. ed incentivi	X		X (>2 anni)		X	X (>1 anno)		X (<1 anno)	X (>1 anno)
		e) divieto di pubblicizzare beni/servizi	X	X	X (>2 anni)	X	X	X (>1 anno)		X (<1 anno)	X (>1 anno)
		c) confisca	X	X	X	X	X	X	X	X	X
		d) pubblicazione della sentenza	possibile se interd.	possibile se interd.	possibile se interd.	possibile se interd.	possibile se interd.	possibile se interd.		possibile se interd.	possibile se interd.

4 ESCLUSIONE DELLA RESPONSABILITÀ AMMINISTRATIVA

Per beneficiare dell'esenzione da responsabilità gli Enti devono elaborare un modello di organizzazione, gestione e controllo tale da rispondere alle esigenze della realtà aziendale di riferimento. In tal senso l'art. 6 del Decreto prevede che l'Ente non risponde se prova che:

- **a.** l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi;
- **b.** il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo interno dotato di autonomi poteri di iniziativa e controllo;
- **c.** le persone fisiche hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- **d.** non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il regime probatorio è differente a seconda che il reato sia stato commesso:

- da un soggetto in posizione apicale (art. 6 D.Lgs. n. 231/01), nel qual caso l'onere della prova dell'idoneità ed efficacia del modello organizzativo è attribuito all'Ente;
- da un soggetto in posizione subordinata (art. 7 D.Lgs. n. 231/01), nel qual caso l'onere della prova è attribuito all'accusa.

Merita evidenziare che l'Ente non risponde quando coloro che hanno commesso uno dei c.d. reati presupposto, hanno agito nell'interesse esclusivo proprio o di terzi (art. 5 comma 2 D.Lgs. n. 231/01) e che la responsabilità dell'Ente è esclusa se, prima della commissione del reato, è stato adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire i reati della specie di quello verificatosi.

Va sottolineato che, allo stato, non esiste una univoca precisazione delle caratteristiche di un Modello di Organizzazione e Gestione pienamente esimente, anche se il D.Lgs. n. 231/01 delinea i seguenti contenuti minimi del Modello che deve:

1) individuare le attività nel cui ambito possono essere commessi i reati;
2) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
3) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello organizzativo;
5) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello organizzativo.

LA REALTA' CONSIDERATA

Acquedotto Poiana s.p.a. è un'azienda a totale partecipazione pubblica (e soggetta a direzione e coordinamento della società CAFC s.p.a.) che si occupa, in *regime in house providing*, della gestione integrata dell'intero ciclo dell'acqua - captazione (il prelievo fisico dell'acqua da sorgenti o pozzi), adduzione (il trasporto dell'acqua prelevata nei serbatoi), distribuzione, vettoriamento (trasporto) acque reflue e depurazione delle stesse - nell'ambito dei seguenti Comuni:

- Cividale del Friuli;
- Buttrio;
- Corno di Rosazzo;
- Manzano;
- Moimacco;
- Pavia di Udine;
- Pradamano;
- Premariacco;
- Remanzacco;
- San Giovanni al Natisone;
- Trivignano Udinese;
- San Pietro al Natisone.

La Società ha sede legale ed amministrativa a Cividale, Viale Duca degli Abruzzi, ma vi sono anche altre sedi operative, ancorché tecniche, e la Società possiede un'altra unità locale, regolarmente denunciata alla CCIAA come deposito, in Cividale in via delle Manifatture n. 14 (un capannone prefabbricato adibito a magazzino).
L'interazione produttiva è assicurata da un Sistema di Gestione Qualità, Ambiente e Sicurezza conforme alle norme UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 e ISO 45001:2018, di seguito per brevità anche solo "SGI".
Per il dettaglio, si rimanda espressamente alla Parte Generale del presente Modello.

LE ATTIVITÀ "SENSIBILI" AI FINI DEL D.LGS. 231/01. SOGGETTI COINVOLTI E DESTINATARI DELLA PRESENTE PARTE SPECIALE

Si designano come **"*attività sensibili*"** specifiche aree di attività di Poiana all'interno delle quali possono essere commessi alcuni dei reati presupposto trattati nella presente Parte Speciale.
L'analisi delle attività della Società ha portato all'individuazione di alcune fasi critiche che possono essere potenzialmente più esposte alla commissione dei reati suddetti e dei soggetti nelle medesime

coinvolti, che devono pertanto considerarsi a tutti gli effetti i principali, ma non esclusivi, destinatari della presente Parte Speciale.
Nel perseguimento delle finalità dell'Ente, i sistemi informativi e gli strumenti informatici rientrano nella gestione contabile ed amministrativa, nelle comunicazioni istituzionali ed operative aziendali ma anche quale repository per la formazione, la conservazione e la catalogazione dei referti analitici e della corrispondenza con private, aziende e enti.
In particolare, si sono considerati anche i processi di eProcurement svolti effettivamente all'interno della Società e si è proceduto ad una loro mappatura, che viene presentata in figura seguente.

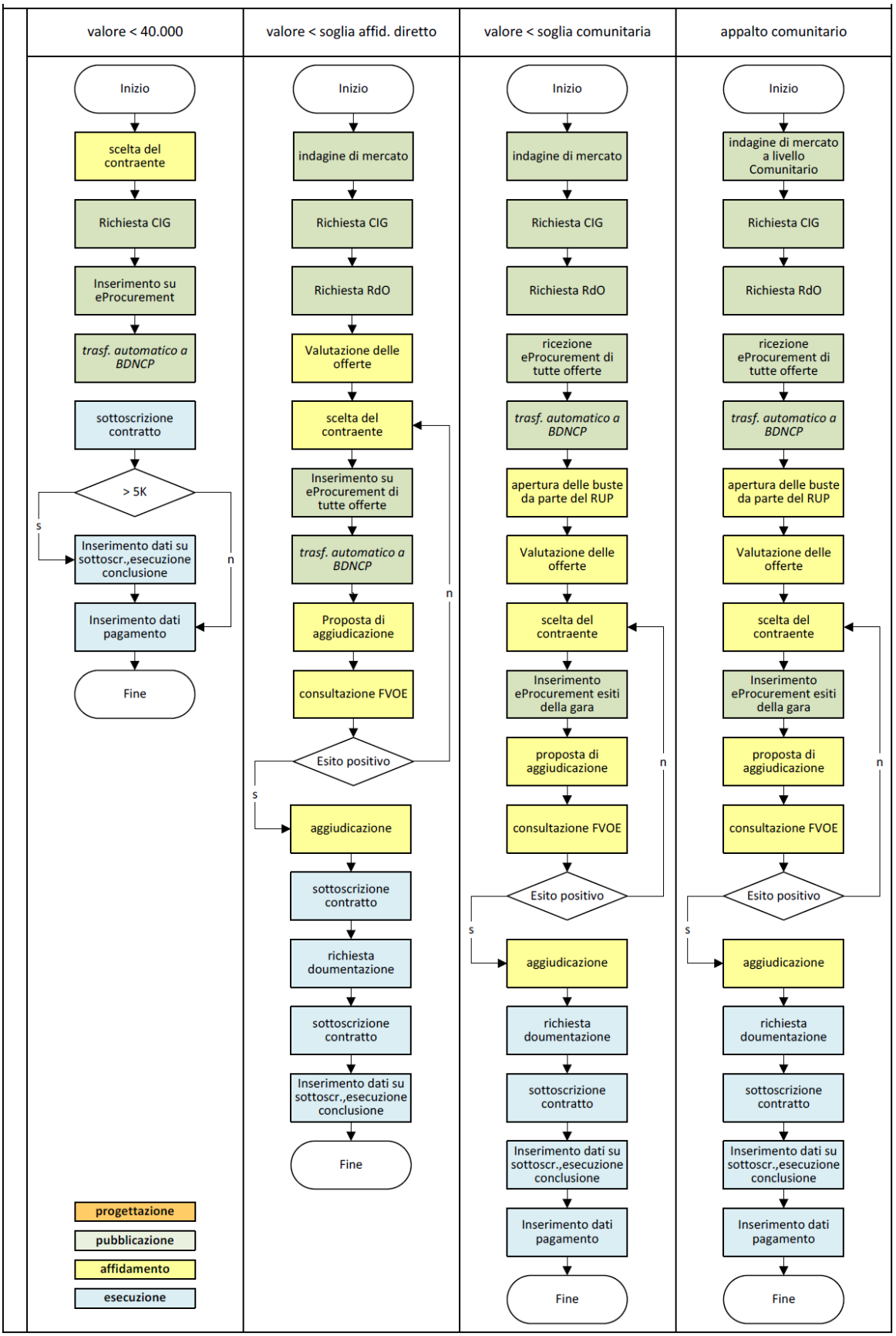

Figura 3 – Processo di eProcurement in funzione degli importi

In maniera integrata, la presente Parte Speciale si preoccupa di definire anche le interrelazioni con l'ambito del trattamento di dati personali, la cui normazione e regolamentazione ha subito recenti modifiche.
In realtà, i reati che afferiscono al trattamento di dati personali non rientrano nell'ambito dei reati presupposto ma, al fine di considerare un insieme di regole coerenti sull'utilizzo dei sistemi informativi, si è deciso di considerare anche questo ambito normativo.
In questa sede basta ricordare che il 4.5.2016 è stato pubblicato il Regolamento UE 2016/679 - "*Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*)". Tale Regolamento, cui ci si riferirà nel prosieguo anche con l'acronimo "*GDPR*" (General Data Protection Regulation), ha il duplice obiettivo di uniformare la declinazione operativa di concetti e principi che rappresentano la logica conseguenza dei valori fondanti l'Unione Europea e quello di ammodernare questi principi a seguito della rivoluzione tecnologica e gestionale che caratterizza la realtà odierna. Sebbene sia ben definita la volontà di tutelare le persone fisiche, esso si applica a tutti i soggetti presenti nell'UE ma anche ai soggetti che non effettuano il trattamento all'interno della UE, se questo è finalizzato:

- all'offerta di beni o la prestazione di servizi ai soggetti interessati;
- al monitoraggio del comportamento degli interessati, nella misura in cui tale comportamento abbia luogo all'interno dell'UE.

Il Regolamento prevede anche una serie di obblighi per le imprese che trattano dati personali, in una ottica di maggiore tutela per gli interessati: vanno in questa direzione l'obbligo di protezione dei dati fin dalla progettazione (*Privacy by Design*) e di protezione per impostazione predefinita (*Privacy by Default*). Il Regolamento sancisce, inoltre, il principio di "*accountability"*, in base al quale è il Titolare a dover dimostrare l'adozione di politiche privacy e misure adeguate conformi al Regolamento, cui è imposto di tenere un "*registro delle attività di trattamento*" svolte sotto la propria responsabilità.
Al "*Titolare*", al "*Responsabile"* già individuate nel D.Lgs. n. 196/03, il GDPR ha affiancato il Data Protection Officer ("*DPO"*), che deve essere nominato:

- nei casi in cui il trattamento venga effettuato da un'autorità pubblica o da un organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);
- qualora le attività principali del Titolare e del Responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- nell'ipotesi in cui le attività principali di suddetti soggetti consistano in trattamenti su larga scala di categorie particolari di dati personali (dati sensibili, dati genetici, biometrici, dati giudiziari).

Il DPO, può essere un dipendente del titolare del trattamento o, in alternativa, assolvere i propri compiti in base ad un contratto di servizi. Da una lettura dell'art. 38, comma 3, si evince che il DPO ha un ruolo di estrema importanza, dovendo riferire direttamente all'Organo Amministrativo o comunque ai vertici gerarchici della società, senza intermediazioni, e con grande autonomia e indipendenza, rispetto agli altri dirigenti.
Tra i suoi doveri rientrano:

- informare e consigliare il Titolare ed il Responsabile del trattamento, nonché i soggetti autorizzati al trattamento, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni vincolanti relative alla protezione dei dati;

- verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri in materia di dati personali, nonché delle politiche del Titolare e del Responsabile del trattamento in materia di protezione dei dati personali (inclusi l'attribuzione delle responsabilità, la sensibilizzazione del personale incaricato e i relativi audit);
- fornire, se richiesti, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
- cooperare e fungere da punto di contatto per il Garante per la protezione dei dati personali e per gli interessati per qualunque problematica relativa al trattamento dei loro dati e all'esercizio dei loro diritti.

Per quanto attiene **l'informativa**, questa deve essere più completa e riportare maggiori dati: ad esempio, deve riportare il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; nel caso in cui esista un processo decisionale automatizzato che riguardi l'interessato, dovrà contenere i dettagli sulla logica utilizzata e le conseguenze di tale trattamento per l'interessato.
Il Regolamento riporta anche specifiche previsioni sui diritti degli interessati già presenti nella Direttiva (trasparenza, accesso e rettifica dei dati personali che li riguardano, trasparenza, opposizione) e ha introdotto nuovi diritti, fra cui il diritto all'oblio e il diritto alla portabilità dei dati.

La fornitura del servizio idrico integrato, interessa sia Aziende (B2B) che privati (B2C).
Nel primo caso, coinvolgendo persone giuridiche, non viene effettuato alcun trattamento di dati personali; nel secondo caso, invece, si trattano dati personali per finalità amministrative/contabili.
L'utilizzo per fini di marketing (invio di mail commerciali) richiede il consenso esplicito anche per le persone giuridiche che possono iscriversi al Registro delle opposizioni.
Oltre alle informative a collaboratori e loro familiari, nonché a professionisti e ditte individuali, deve essere gestita la problematica dei *Cookies*, per i quali è necessario stendere adeguata informativa e chiedere il consenso: ogni volta che un sito ne fa potenzialmente uso, è necessario avvisare l'utente ed informarlo sulla natura dei cookies che, nel caso di specie, dovrebbero essere meramente tecnici e non di profilazione anche se è presente l'informativa come link e non come popup.
Dal punto di vista attivo: i soggetti esterni debbono essere nominati Responsabili, mentre gli interni debbono essere esplicitamente autorizzati per poter legittimamente trattare i dati.

La figura che segue mostra i soggetti con un ruolo attivo e gli interessati del trattamento.

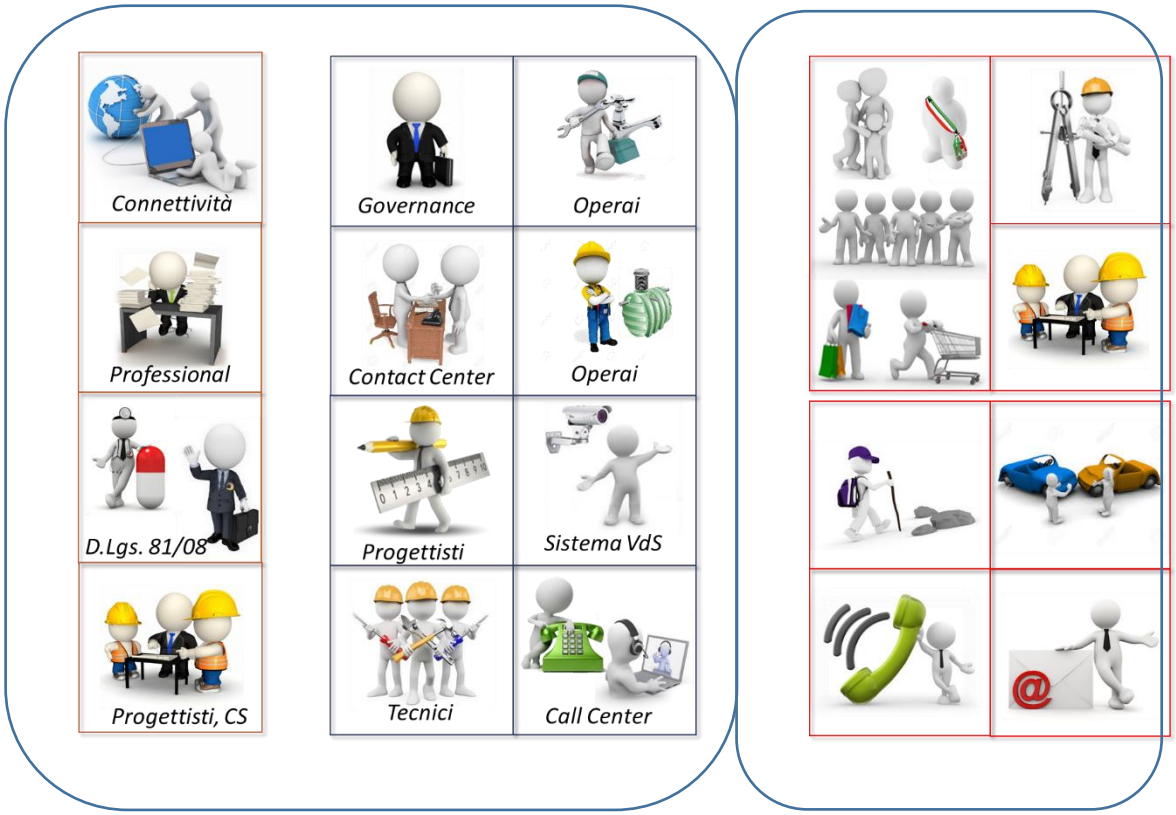

Figura 4 – Figure e ruoli nel trattamento dati

Di seguito, si riepilogano i reati di interesse:

24 bis	**Art. C.P.**	**Note**
Accesso abusivo ad un sistema informatico o telematico.	615 ter	Rientrano in quest'ambito: • azioni di attacco/sabotaggio a sistemi informativi di enti di controllo; • alterazione di dati di fornitori/outsourcer di servizi; • alterazione di dati contabili interni; • falsificazione degli esiti analitici o di documenti; • un apicale od un collaboratore subordinato che svolge attività di intelligence che porti l'Ente a conoscere dati ed informazioni che l'Ente può sfruttare per ottenere un vantaggio; • un soggetto che effettua un'estorsione i cui effetti provocano un vantaggio all'ente, utilizzando o compromettendo strumenti informatici o telematici
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	617-quater	
Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	617-quinquies	
Danneggiamento di informazioni, dati e programmi informatici	635-bis	
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	635-ter	
Danneggiamento di sistemi informatici o telematici	635-quater	
Danneggiamento di sistemi informatici o telematici di pubblica utilità	635-quinquies	
Estorsione	629	
Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici	615 quater	
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informativo o telematico	635-quater.1	
Falsità di documenti informatici.	491 bis	
Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	640-quinquies	
24 c.1	**Art. C.P.**	
Frode informatica (in danno dello Stato o di altro Ente pubblico)	640 ter	Rientrano in quest'ambito: • Frodi in danno di pubbliche amministrazioni; • Turbativa nella scelta di fornitori ed outsourcer; • Soppressione di documenti relativi a forniture.
Turbata libertà degli incanti	353	
Turbata libertà del procedimento di scelta del contraente	353-bis	
Frode nelle pubbliche forniture	356	
25 quinquies c.1 lett. b (da 300 a 800 quote)	**Art. C.P.**	
Induzione, favoreggiamento o sfruttamento della prostituzione	600 bis	Rientrano in quest'ambito:

minorile	c.1	• l'utilizzo (come merce di scambio) della prostituzione minorile a mezzo telematico; • la generazione di contatti fra membri di questo tipo di community;
Realizzazione di esibizioni pornografiche con minori; produzione di materiale pornografico con minori; induzione alla partecipazione di minori ad esibizioni pornografiche.	600 ter c.1	Rientrano in quest'ambito: • la realizzazione (come merce di scambio) di materiale legato a pornografia minorile (anche virtuale)
Commercio di materiale pornografico cui partecipano minori.	600 ter c.2	
Compimento di atti sessuali con un minore	600 bis c.2	
Distribuzione, divulgazione, diffusione e pubblicizzazione anche per via telematica, di materiale pornografico con minori; Divulgazione di notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori	600 ter c.3	
Offerta e/o cessione di materiale pornografico cui partecipano minori.	600 ter c.4	
Acquisizione e detenzione di materiale pornografico realizzato utilizzando minori	600 quater	
25 novies (fino a 500 quote)	**art L.633**	
Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa. Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione.	171 c.1 lett. a-bis) e 171 c.3	Rientrano in quest'ambito: • utilizzo come merce di scambio
Importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di Software. Azioni atte a consentire o facilitare la rimozione arbitraria o	171 bis	Rientrano in quest'ambito: • l'utilizzo di software non originale (anche per situazioni BYOD o su Elaboratori ed attrezzature personali) o in violazione degli

l'elusione funzionale di dispositivi applicati a protezione di Software. Violazione diritto d'autore in relazione a banche dati.		accordi di licenza (underlicencing, downgrade di versioni, sprotetto per l'interfaccia con altri software); • la presenza di banche dati clonate;
Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico di opere dell'ingegno	171 ter	Rientrano in quest'ambito: • la diffusione in ambiente di lavoro di musica, film ed altro materiale protetto dal diritto d'autore; • l'utilizzo come merce di scambio
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione.	171 septies	N.A.
Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.	171 octies	Rientrano in quest'ambito: • l'utilizzo come merce di scambio

5 IL SISTEMA DEI CONTROLLI

La prevenzione dei reati in ambito informatico non può prescindere dalla piena consapevolezza che il sistema informativo aziendale, è in realtà, qualcosa di più complesso di un sistema informatico e, nella trattazione che segue, ci si riferisce alla concettualizzazione del Sistema Informativo come composto da 5 componenti.
In questa visione, un sistema informativo è costituito, infatti, dai seguenti elementi: gli **strumenti** (HW e SW), gli **utilizzatori del sistema**, il **dataset**, le **procedure elaborative**, i **valori di riferimento** che l'Ente si è data come principi guida.

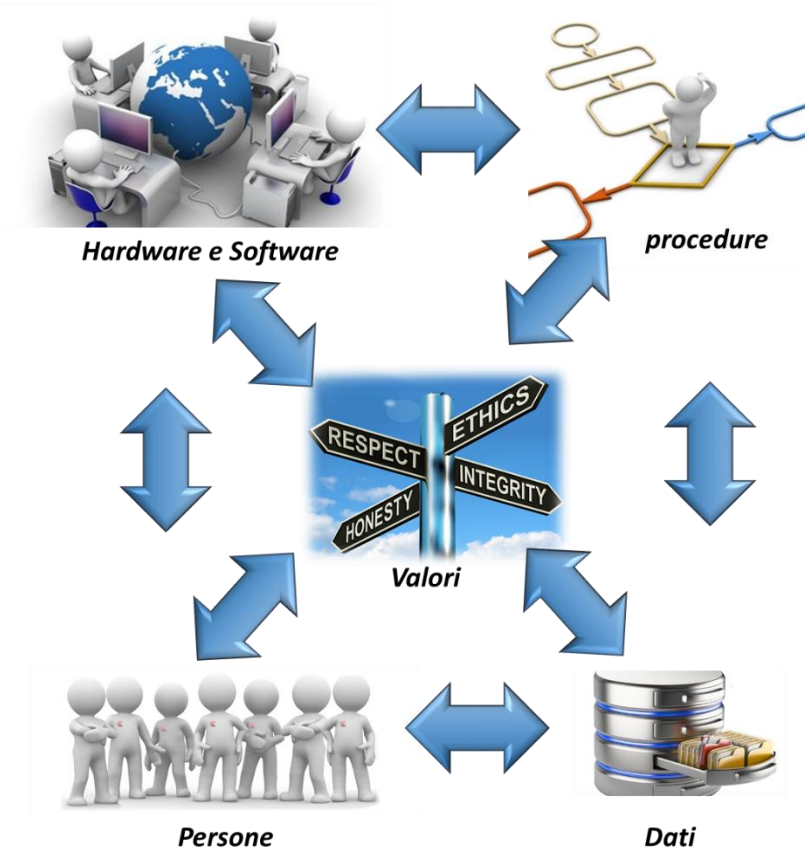

Figura 3

Pertanto, per impedire la commissione di reati presupposto è necessario agire intervenendo su tutte e cinque le componenti e, per farlo, si è tenuto conto dei seguenti indirizzi:

- delle previsioni del D.Lgs. n. 231/2001;
- della vigente disciplina legislativa in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679 e del D. Lgs. 196/2003, come modificato dal D.Lgs. 101/2018;
- dei provvedimenti e delle indicazioni del Garante per la Protezione dei Dati Personali;
- della vigente disciplina legislativa di cui al Codice penale e alle norme speciali di settore;

- del D.M. 13/02/2014 – "*Procedure semplificate per l'adozione dei modelli di organizzazione e gestione nelle piccole e medie imprese*";
- delle "*Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n°231/2001*" redatte da Confindustria (edizione marzo 2014, approvate dal Ministero della Giustizia in data 21 luglio 2014, e edizione giugno 2021);
- dei "*Principi di redazione dei Modelli di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001*" elaborato nel giugno 2016 dal Comitato tecnico-scientifico "*Linee Guida per la redazione e l'attestazione dei modelli organizzativi ex D.lgs. 8 giugno 2001, n. 231*" costituito in seno al Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili e dei "*Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del d.lgs. 8 giugno 2001, n. 231*" pubblicati nel febbraio 2019.

Nel prosieguo si presenteranno le contromisure di cui Acquedotto Poiana s.p.a. si è dotata, articolate in relazione alle componenti del sistema informativo.

5.1 Valori condivisi: il Codice Etico.

Acquedotto Poiana s.p.a. offre e gestisce un servizio pubblico di interesse economico.
I processi utilizzano dati personali e strumenti elettronici per il trattamento, per i quali risulta imprescindibile la stesura di regole, protocolli comportamentali e procedure ed indispensabile ed inderogabile fornire a tutti i collaboratori e partner un set di valori a cui, questi ultimi, possono ispirare il loro comportamento.
Acquedotto Poiana s.p.a. si è dotata di un proprio Codice Etico allineato alle norme del Codice di Comportamento di cui al D.P.R. 16.04.2013 n. 62 (per come, da ultimo, modificato dal D.P.R. 13.06.2023 n. 81)[14] di applicazione generale a tutte le pubbliche amministrazioni, cui Acquedotto Poiana s.p.a. si conforma per quanto compatibili, altresì attenendosi ai contenuti minimi del *"Codice di Comportamento delle Imprese e degli Enti di Gestione dei Servizi Pubblici Locali"* redatto da Confservizi[15].
Il Codice Etico di Acquedotto Poiana s.p.a. integra, ai sensi dell'articolo 54 del D.Lgs. n. 165/2001 e della deliberazione ANAC n. 177/2020 ("*Linee guida in materia di Codici di comportamento delle amministrazioni pubbliche*") le previsioni del Codice di comportamento dei dipendenti pubblici che ha definito i doveri minimi di diligenza, lealtà, imparzialità e buona condotta che i dipendenti pubblici sono tenuti ad osservare e che, per quanto compatibili, si estendono ai dipendenti di Acquedotto Poiana s.p.a..
In particolare, al fine di prevenire, ed impedire il verificarsi degli illeciti ricollegabili al Sistema Informativo, tutti i destinatari del modello debbono:

- rispettare le Leggi e Regolamenti a livello Europeo, Statale, Regionale e Locale;
- rispettare i principi di:
  - Legalità ed Integrità: rispetto di leggi, regolamenti ma anche integrità morale;
  - Correttezza, lealtà ed onestà: rapporti corretti con tutti gli interlocutori, cui fornire tutti gli elementi per scegliere ed agire liberamente ed in maniera informata;

[14] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:2013-04-16;62
[15] In ottemperanza a quanto disposto dall'art. 5 del D.M. 201/2003, tale documento ha ottenuto parere favorevole in merito alla sua idoneità da parte del Ministero della Giustizia

- Fedeltà e Prevenzione del conflitto di interessi: l'interesse primario e superiore del bene aziendale non deve essere messo a rischio da fenomeni opportunistici;
- Lotta alla Corruzione e Trasparenza: il rispetto delle regole non deve essere messo in discussione e la trasparenza sull'agire di ogni apicale, collaboratore o partner debbono garantire un controllo "diffuso";
- Valorizzazione delle risorse umane: Le risorse umane sono uno degli asset più importanti e, come tale, vanno valorizzate;
- Data Protection e Riservatezza: deve essere garantita la massima riservatezza e la possibilità di controllo da parte degli "interessati";
- Tutela dell'immagine aziendale: anche l'immagine aziendale è un asset di rilievo, proprio in virtù di essere fornitori di un servizio pubblico che impiega una risorsa pubblica;
- Imparzialità ed assenza di discriminazioni: razza, sesso, abitudini sessuali, credo politici e religiosi non possono costituire basi per discriminare risorse interne e stakeholder;
- Tutela ambientale e della salute: il rispetto dell'ambiente e della salute umana di tutti gli stakeholder vengono prima di ogni altra cosa e debbono guidare nelle scelte aziendali.
- Rispetto dei valori democratici: la politica non deve influenzare l'azione aziendale

Per quanto sopra, in relazione ai sistemi informativi, ogni destinatario, in linea di principio:

- è responsabile della sicurezza dei sistemi utilizzati ed è soggetto alle disposizioni normative in vigore e alle condizioni dei contratti di licenza;
- non è autorizzato ad utilizzare per fini diversi da quelli inerenti al rapporto di lavoro o per inviare messaggi offensivi o che possano arrecare danno all'immagine dell'impresa gli strumenti messi a disposizione;
- è tenuto a prestare il necessario impegno al fine di prevenire la possibile commissione di reati mediante l'uso degli strumenti informatici, riferendo con tempestività e riservatezza al proprio responsabile ed all'Organismo di Vigilanza di ogni notizia di cui sia venuto a conoscenza nell'espletamento della propria attività lavorativa, circa violazioni di norme giuridiche, del Codice Etico o di altre disposizioni aziendali che possano, a qualunque titolo, coinvolgere la Società;
- è tenuto al rispetto delle procedure legate ad un utilizzo improprio dei dati, nel pieno rispetto delle norme a tutela della privacy, in base alle quali, deve, altresì, custodire con cura gli atti affidatigli;
- è tenuto alla massima riservatezza nella gestione delle informazioni apprese nell'esercizio delle proprie funzioni in conformità alla Legge, ai regolamenti e alle circostanze, anche dopo la cessazione del rapporto di lavoro.

5.2 Protezioni Hardware e Software

Per rispondere ai dettami normativi in materia di trattamento dati, nonchè ai disposti di cui all'art. 32 del GDPR - ed anche in relazione alla Direttiva 2022/2555 ("*Direttiva NIS2*"), alla Direttiva 2022/2557 ("*Direttiva CER*" sulla resilienza delle infrastrutture critiche), alla Direttiva 2022/2184 recepita dal D.Lgs. n. 18/2023 ("*Piano di sicurezza dell'acqua*") e al Reg. 2023/2841 ("*Regolamento sulla*

Cyberiscurezza") e s.m.i. - Poiana ha adottato opportune misure di sicurezza organizzative, procedurali e tecniche.[16]
In sintesi, è stato definito un sistema di autorizzazione formale al trattamento, associato ad un processo di autenticazione mediante opportune credenziali, periodicamente aggiornate. Per ciascuno dei collaboratori è stato previsto il rilascio di istruzioni ed è stato svolto un percorso formativo, ripetuto con scadenze regolari. Si è proceduto alla segmentazione e compartimentazione della rete, riducendo i single point of failure.
La struttura si è dotata di un sistema antimalware costantemente aggiornato e di firewall.
Il patching è un processo di routine e si è cercata la ridondanza.
Il backup dei dati avviene con frequenza superiore a quella imposta dalla Legge ed il funzionamento del sistema viene garantito con gruppi di continuità. Le politiche di backup garantiscono il Recovery del S.I..

5.3 La Policy sul trattamento dati e sull'utilizzo degli strumenti

Poiana si è dotata di una Policy dal titolo "*Utilizzo consapevole degli strumenti informatici*", approvata dall'Organo amministrativo e che costituisce parte integrante della presente Parte Speciale.
Tale Policy è stata sviluppata per disciplinare in maniera organica l'utilizzo dei sistemi di elaborazione delle informazioni ed il trattamento di dati, coerentemente con i disposti legati alla normativa nazionale ed europea (Regolamento (EU) 2016/679, D.Lgs. n. 196/03 e s.m.i.).
Le indicazioni contenute nel documento sono valide anche per ciò che attiene la prevenzione dei reati di cui al D.Lgs. n. 231/2001.
I contenuti della Policy sono riassunti sinteticamente nella tabella che segue:

Riferimento	Contenuto
1- Premessa	Richiamo sulla necessità di una Policy.
2- Rapporto fra Collaboratori ed Ente	Definizioni per meglio comprendere il contenuto.
3- Valori ed Obiettivi sociali	Poteri e Responsabilità
4- Business Compliance	• Comportamenti per prevenire la Responsabilità Amministrativa degli Enti; • Pornografia e pedopornografia; • Diritto d'Autore
5- Sicurezza	La sicurezza di dati e strumenti
6- Utilizzo di strumenti aziendali	Modalità e limitazioni nell'utilizzo degli asset aziendali.
7- Controlli	Modalità di effettuazione dei controlli.

[16] **Riservandosi di adempiere alle previsioni di cui alla Legge n. 90 del 28.06.2024 (rubricata *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici")* nei termini e modalità ivi previsti e per come verranno disciplinati dai previsti provvedimenti attuativi.**

Si precisa che dati e strumenti sono destinati ad un uso aziendale interno alla struttura, legato alla propria mansione, e ne è vietato l'uso personale anche per una archiviazione temporanea di file.
Coerentemente con i valori del Codice Etico, è vietata la detenzione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica e di materiale pornografico. Stante la natura professionale dei dati e degli strumenti, la Società ha la possibilità di accedere agli archivi informatici, compresi gli archivi di posta elettronica. Non è consentita l'attivazione di sistemi di protezione autonomi (password di protezione delle cartelle, …) senza preventiva autorizzazione scritta.
Gli strumenti assegnati in uso debbono essere custoditi con la diligenza del buon padre di famiglia e, soprattutto, mantenuti sempre in efficienza: eventuali anomalie, i guasti o i malfunzionamenti debbono essere segnalati.
Gli unici programmi eseguibili sono quelli forniti da Acquedotto Poiana s.p.a. e non è consentito l'utilizzo di programmi diversi (anche se residenti su supporto rimovibile). Si ricorda che l'utilizzo di SW è soggetto al diritto d'autore le cui violazioni possono portare a sanzioni penali significative, sanzioni amministrative ed al risarcimento dei danni anche morali richiesti dal detentore dei diritti.
La Policy contiene, infine, prescrizioni specifiche che prescrivano a ciascun addetto di:

- astenersi dalla falsificazione di qualsiasi documento informatico;
- astenersi dall'effettuare accessi abusivi o mantenersi in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso;
- astenersi dal detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici;
- non configurare l'accesso remoto al Sistema Informativo di Acquedotto Poiana s.p.a. su computer diversi da quello in uso;
- non consentire a chiunque esterno a Poiana di collegare il proprio computer alla rete aziendale senza previa autorizzazione dell'Organo Amministrativo e/o del Direttore Generale della Società;
- non usare né diffondere apparecchiature, dispositivi o programmi informatici che possano in qualsiasi modo danneggiare o interrompere un sistema informatico o telematico;
- astenersi dal rivelare, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni fraudolentemente intercettate relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- astenersi dall'intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche e dall'utilizzare dispositivi tecnici o strumenti software apparecchiature idonee ad intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- astenersi dal distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o della Società;
- astenersi dal distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o della Società o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- non effettuare alcuna attività rivolta al danneggiamento di informazioni, dati e programmi informatici o al danneggiamento di sistemi informatici e telematici;
- non formare o trasmettere un documento informatico falso ovvero alterare un documento informatico vero;

- non alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- astenersi scrupolosamente alle istruzioni operative e alle procedure aziendali diffuse e in uso presso Acquedotto Poiana s.p.a.;
- evitare di condividere documenti e file in genere con il computer personale o di altri;
- avvisare immediatamente l'Organo Amministrativo e/o il Direttore Generale della Società qualora sia notato personale presumibilmente non autorizzato che movimenta i cavi di rete, collega apparati di qualunque tipo alla rete informatica e/o telefonica, oppure accede ai locali tecnici;
- avvisare immediatamente l'Organo Amministrativo e/o il Direttore Generale della Società qualora venga indebitamente sottratto il proprio computer o qualsiasi altro dispositivo utilizzato per connettersi alla rete di Acquedotto Poiana s.p.a..

5.3.1 L'organizzazione interna e l'organizzazione esterna

All'interno della Società, esiste una macrostruttura (descritta dall'Organigramma) ed una microstruttura (descritta dal mansionario) coerente con le dimensioni e con il particolare settore nel quale si trova ad operare.
L'organigramma aziendale, per ciò che attiene la tematica Privacy e Trattamento dati, è presentato in figura seguente.

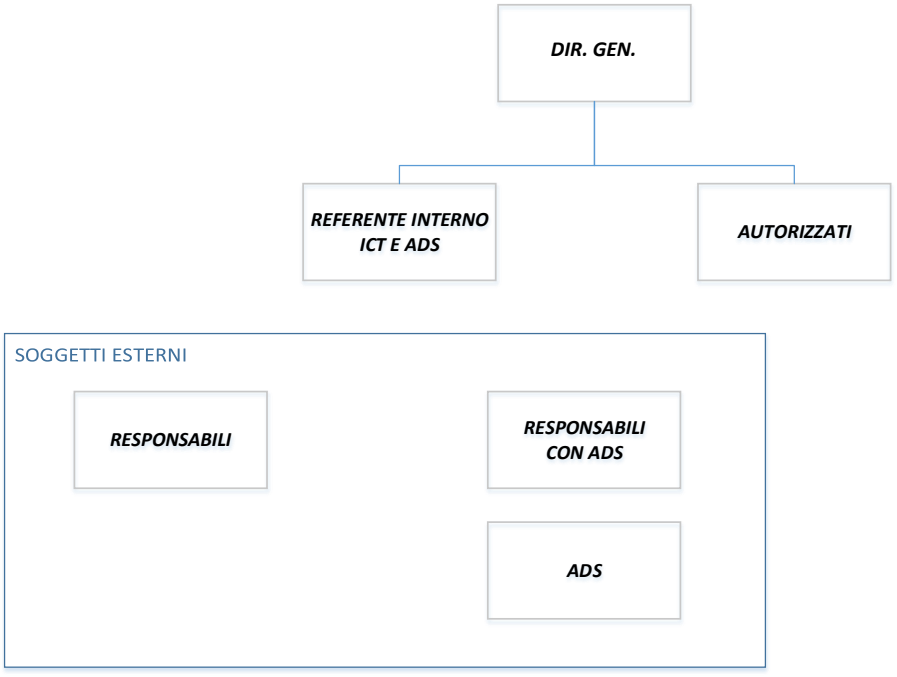

Figura 4

Stanti le ridotte dimensioni, non esiste una funzione strutturata che si occupa dei "*Sistemi Informativi*" ma esiste un referente interno cui sono state assegnate mansioni specifiche.

L'Organo Amministrativo ha provveduto a formalizzare una delega alla Direzione Generale (Delegato) che, direttamente o tramite soggetti incaricati, redige (e manutiene) un documento nel quale, oltre alla descrizione del materiale informatico presente in azienda, indica per ciascun collaboratore le dotazioni rispettivamente assegnate.

Il Delegato cura che sia impartita a tutti i dipendenti e collaboratori della Società una adeguata formazione tecnica sull'utilizzo della strumentazione informatica e sulle regole comportamentali e procedurali a cui si devono attenere, sui contenuti del D.Lgs. n. 231/2001 e dei reati correlati: tutti i dipendenti e collaboratori sono a conoscenza delle istruzioni operative adottate da Acquedotto Poiana s.p.a. in merito all'utilizzo di sistemi informatici, nonché dei Protocolli.
La formazione è prevista in fase di assunzione (e/o di cambio mansioni) e viene ripetuta con cadenza almeno annuale in ordine alle novità legislative ed ai controlli previsti dal Modello.

I server aziendali si trovano sia presso la sede aziendale, sono collocati in locali protetti e l'accesso è consentito solo ai tecnici IT delle ditte incaricate; inoltre esistono contratti per la fornitura di servizi Cloud, stipulati con primari interlocutori. Nell'ambito di Poiana i soggetti autorizzati alla firma custodiscono personalmente il proprio dispositivo di firma.

5.3.2 Hardware, Software e Servizi a Valore Aggiunto

L'istallazione di nuove apparecchiature IT o la creazione/modifica di procedure deve essere formalmente approvata. L'approvazione include il parere favorevole del Direttore Generale quale Delegato che, direttamente o tramite soggetto incaricato, ne ha autorizzato l'acquisto.
Il processo di definizione ed approvazione di nuove strutture IT, e della loro modifica, è sempre formalizzato in esito ad un'analisi avente come finalità quella di assicurare che le nuove tecnologie/risorse/strutture informatiche HW o SW non presentino lacune sotto il profilo della sicurezza e non influenzino negativamente i sistemi e le procedure precedentemente presenti.
Il citato Delegato è informato di problemi ai sistemi di elaborazione, per verificare che la sicurezza del patrimonio informativo non sia stata pregiudicata e ogni evento rilevante viene documentato (ad esempio mediante la compilazione di un "*ICT Storyboard*"): ciò consente di ottenere dati statistici circa l'occorrenza e la frequenza di determinati problemi, le migliori azioni da adottare e la pianificazione futura delle risorse informatiche.
Nel caso di connessioni con sistemi di terzi, deve essere prevista nei contratti con terze parti l'introduzione di specifiche clausole a previsione delle politiche e procedure di sicurezza informatica volte a prevenire i rischi.
Nel caso di contratti in outsourcing per servizi informatici deve essere previsto l'inserimento di clausole formalizzate che consentano alla Società di svolgere audit in materia di sicurezza informatica presso l'outsourcer stesso.

5.3.3 L'Organismo di Vigilanza

L'Organismo di Vigilanza (di seguito OdV) - fermo quanto previsto dalla Policy Whistleblowing adottata dalla società e dal proprio Statuto - ha il compito di vigilare "*sul funzionamento e sull'osservanza del Modello stesso e di curarne l'aggiornamento*"(art. 6 comma 1 lettera b) del D.Lgs. n. 231/2001 e s.m.i.). Nei confronti di tale Organismo sono istituiti degli *obblighi di informazione* (art. 6, comma 2 lettera d), del D.Lgs. n. 231/2001 e s.m.i.) che riguardano la trasmissione di informazioni utili ai fini dello svolgimento di tale attività di vigilanza.

All'Organismo di Vigilanza, secondo quanto previsto dal relativo Statuto, oltre alla facoltà di attivarsi con specifici controlli in seguito alle segnalazioni ricevute, spetta il potere di effettuare controlli a campione (anche a sorpresa) volti alla verifica della corretta osservanza dei principi e delle regole espressi dalla presente Parte Speciale, nonché dai documenti dalla stessa richiamati.

L'OdV ha facoltà di accedere a tutta la documentazione relativa alla gestione amministrativa, economica e finanziaria, ed in particolare ai rapporti della Società con gli Enti di Controllo e i pubblici ufficiali/incaricati di pubblico servizio in genere, nonché la facoltà di accedere presso le sedi sociali e tutti i locali ove si svolga l'attività di Società.

Per consentire l'efficacia del Modello 231 della Società, fermo quanto previsto nella Parte Generale e nella Policy Whistleblowing adottata dalla Società stessa, l'Organismo di Vigilanza deve essere opportunamente informato in base ai flussi previsti dallo Statuto dell'OdV e dalla presente Parte Speciale.
Tra i compiti dell'Organismo di Vigilanza rientrano:

- verificare costantemente la completezza e l'efficacia delle disposizioni della presente Parte Speciale;
- svolgere ogni accertamento ritenuto opportuno su singole operazioni o in relazione al flusso informativo;
- svolgere verifiche periodiche sul rispetto delle procedure interne e del "sistema" di controllo in ambito informatico, sul diritto d'autore e la prevenzione dei reati a sfondo pornografico e pedopornografico;
- indicare al management ogni opportuna modifica e innovazione nelle procedure aziendali, volte a un a migliore prevenzione del rischio di commissione di reati;
- esaminare eventuali segnalazioni specifiche di anomalie ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.
- verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole standard finalizzate:
    - o all'osservanza da parte dei Destinatari dei contenuti del Modello e del Codice Etico;
    - o alla possibilità di Acquedotto Poiana s.p.a. di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
    - o all'attuazione di meccanismi sanzionatori (quali la risoluzione del contratto nei riguardi di Fornitori, Appaltatori, Consulenti e Outsourcer in materia di sistemi informatici) qualora si accertino violazioni delle prescrizioni.
- accertare ogni eventuale violazione della presente Parte Speciale e proporre eventuali sanzioni disciplinari.

Tra le funzioni peculiari dell'Organismo in relazione alla presente Parte Speciale si segnala:

- verifiche documentali, sia periodiche che a campione;
- valutazione dell'efficacia delle procedure in essere e, se del caso, richiesta di nuove procedure;
- esame di eventuali segnalazioni.

L'OdV riferisce in merito ad ispezioni, controlli, segnalazioni e provvedimenti al Consiglio di Amministrazione / Amministratore Delegato e - in ipotesi di conflitto di interessi – al Collegio Sindacale ovvero alla Assemblea dei soci.
In caso di violazione delle norme di legge e/o dei protocolli aziendali previsti a tutela della corretta gestione aziendale da parte di uno dei soggetti destinatari della presente Parte Speciale, l'Organismo di Vigilanza ha l'obbligo di informare tempestivamente il Consiglio di Amministrazione / Amministratore Delegato e - in ipotesi di conflitto di interessi – al Collegio Sindacale ovvero la

Assemblea dei soci, al fine di permettere agli stessi di agire, assumendo i provvedimenti ritenuti opportuni.
L'Organismo di Vigilanza è tenuto a collaborare con il Responsabile per la Prevenzione della Corruzione e della Trasparenza (di seguito "RPCT") di Acquedotto Poiana s.p.a. - designato come destinatario delle segnalazioni ai sensi del D.Lgs n. 24 del 10.03.2023 - nel rispetto della Policy Whistleblowing e dello Statuto dell'Organismo di Vigilanza della Società cui si rimanda esplicitamente.
Come previsto dalla Parte Generale del Modello Organizzativo di Società - fermo quanto previsto specificatamente nella Policy Whistleblowing - le segnalazioni e i report possono essere inoltrati ed inviati all'Organismo di Vigilanza attraverso l'indirizzo di posta elettronica odv@poiana.it o in qualsiasi forma il segnalante ritenga opportuna.
Per consentire l'efficacia del presente Modello - fermo quanto previsto specificatamente nella Parte Generale, nella Policy Whistleblowing e nello Statuto dell'Organismo di Vigilanza - nella tabella seguente sono riportati alcuni aspetti da comunicare tempestivamente all'OdV con le rispettive periodicità.

All'Organismo di Vigilanza devono obbligatoriamente essere inviate le informazioni previste dalla seguente tabella. Si precisa, in ogni caso, che tutte le comunicazioni annuali debbono essere inviate all'OdV entro il 31 marzo di ogni anno, mentre le comunicazioni ad evento debbono essere inviate entro 30 giorni dall'evento stesso, salvo casi di urgenza ed indifferibilità, rimessi alla valutazione del responsabile della funzione o del segnalante.

Nel caso in cui non si siano verificati eventi nel corso dell'anno, il soggetto incaricato dovrà comunque inviare, almeno una volta all'anno ed entro il 31/03 di ogni anno, una comunicazione all'OdV evidenziando l'assenza di eventi alla voce specifica (a seconda dei casi, ad esempio "*nessun evento*" oppure "*nessuna modifica apportata*").

REPORTING OBBLIGATORIO VERSO L'ORGANISMO DI VIGILANZA			
flusso informativo verso l'OdV		**soggetti coinvolti**	**periodicità**
1	Modifiche nelle Responsabilità e nelle deleghe e nella struttura di Governance	CDA/DELEGATO	AD EVENTO
2	Comunicazioni delle Autorità inerenti il sistema informativo come obiettivo di un reato, come mezzo per compiere reati informatici o come strumento per compiere reati di altra natura	CDA/DELEGATO	AD EVENTO
4	Evento, situazione, condizione che compromette la capacità di elaborazione	DELEGATO	AD EVENTO

REPORTING OBBLIGATORIO VERSO L'ORGANISMO DI VIGILANZA			
flusso informativo verso l'OdV		**soggetti coinvolti**	**periodicità**
5	Mappatura del Sistema Informativo	DELEGATO	AD EVENTO
6	Sistema di Autorizzazione al trattamento	DELEGATO	AD EVENTO
7	Modifiche nei software gestionali	DELEGATO	ANNUALE

5.3.4 Riepilogo sistema dei Controlli

La tabella che segue fa riferimento al sistema dei protocolli adottati per prevenire la commissione dei reati presupposto.

Possibile problematica	Protocolli preventivi
Reati Informatici Turbata libertà del procedimento di scelta del contraente / Frode nelle forniture Pornografia minorile e pedopornografia Violazione diritto d'autore	• *Piano Anticorruzione*; • *Codice Etico*; • Esecuzione e Supervisione a soggetti diversi; • Adozione di misure di sicurezza (sistema di autorizzazione; qualificazione; Antimalware; Firewall; Backup; Credenziali di Autenticazione; Dichiarazione di Conformità;…) & relative agli Amministratori di Sistema (logging, conservazione log, audit log); • Policy "*Utilizzo consapevole degli strumenti informatici*"; • Policy *di Data Breach*; • Policy *Whistleblowing*; • Documento di Tracciatura Dispositivi ed Assegnatari; • Formazione / Informazione; • Autorizzazione per acquisto, installazione e/o modifiche del processo da parte del Delegato; • Predisposizione ICT Storyboard;

	• Inserimento di clausole contrattuali *ad hoc* nell'ambito dei contratti o degli incarichi per i servizi forniti da terzi; • Controlli previsti nelle altre parti speciali; • Audit indipendenti da parte dell'OdV, del Collegio Sindacale e del RPCT; • Giustificabilità degli algoritmi; • Accountability.

6 INTERAZIONE CON ALTRI REATI PRESUPPOSTO

Gli asset informatici costituiscono spesso uno strumento per perpetrare reati ricadenti in altre aree di rischio: grazie agli strumenti informatici, ad esempio, è possibile falsificare documenti, autorizzazioni allo smaltimento dei rifiuti, ddt, fatture etc., e la posta elettronica può costituire lo strumento principe nella comunicazione alla base nelle attività di crimine organizzato o nelle attività corruttive.
E', pertanto, impossibile prevenire dettagliatamente ogni reato prescrivendo contromisure in ambito informatico. Il ruolo prevenzionale è affidato, quindi, al Codice Etico e ad una serie di misure che ricadono nelle singole classi di reato.
I Destinatari dei reati trattati nella presente Parte Speciale in alcune circostanze possono incorrere nel rischio di commissione di altre tipologie di reato.
In particolare, sono state individuate le seguenti frequenti interazioni con altri reati previsti dal D.Lgs n. 231/2001 e si rimanda alle relative Parti Speciali di cui al presente Modello per i principi di comportamento e i sistemi di controllo attuati.

7.1 Reati di cui all'art. 24 D.Lgs. 231/01

L'articolo 24 sanziona i reati di *"Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico*".
In concreto tali ipotesi di reato potranno concorrere con le fattispecie delittuose previste dall'art. 24bis quale fondamento della responsabilità amministrativa dell'Ente quando, per esempio, l'ottenimento indebito di finanziamenti e/o altre erogazioni dallo Stato o da altri enti pubblici sia ottenuto alterando le procedure selettive di evidenza pubblica mediante l'intervento fraudolento sul sistema informatico, l'applicativo, gli algoritmi e/o altri sistemi automatizzati di valutazione delle domande e dei requisiti di partecipazione.
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.2 Reati di cui all'art. 25 D.Lgs. 231/01

L'articolo 25 sanziona i reati di "*Concussione, induzione indebita a dare o promettere utilità e corruzione*" commessi nell'interesse e a vantaggio dell'Ente.
In concreto tali ipotesi di reato potranno concorrere con le fattispecie delittuose previste dall'art. 24 bis (e dall'art. 25 quinquies) quale fondamento della responsabilità amministrativa dell'Ente quando,

per esempio, nel patto corruttivo l'utilità data o promessa al pubblico ufficiale consista in materiale pedopornografico ottenuto e trattato per mezzo di strumenti informatici, ovvero la corresponsione del prezzo della corruzione avvenisse sfruttando sofisticati canali di transazione virtuale.
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.3 Reati di cui all'art. 25 ter D.Lgs. 231/01

L'articolo 25 ter sanziona i delitti societari commessi nell'interesse e a vantaggio dell'Ente.
Concretamente tale disposizione potrà interagire con l'art. 24-bis in discorso laddove, per esempio, le condotte di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 cod. civ.) si attuassero per mezzo di un intervento sui sistemi informativi, i data base ovvero altri applicativi utilizzati dalle autorità di vigilanza medesime.
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.4 Reati di cui all'art. 25 octies D.Lgs. 231/01

L'articolo 25 *octies* prevede che l'Ente risponda per le condotte di "*ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio*" commesse nel proprio interesse.
In concreto tali ipotesi di reato potranno concorrere con le fattispecie delittuose previste dall'art. 24-bis quale fondamento della responsabilità amministrativa dell'Ente quando, per esempio, le disponibilità provenienti da illeciti e reimpiegate vengano fatte passare attraverso transazioni dematerializzate (si pensi al tema delle criptovalute e della blockchain) che prevedono l'utilizzo di strumenti informatici.
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.5 Reati di cui all'art. 25 decies D.Lgs. 231/01

L'articolo 25 *decies* sanziona la commissione nell'interesse o a vantaggio dell'Ente del delitto di cui all'art. 377 bis c.p..
In concreto tali ipotesi di reato potranno concorrere con le fattispecie delittuose previste dall'art. 24 bis e 25 quinquies quale fondamento della responsabilità amministrativa dell'Ente quando, per esempio, la condotta di indurre taluno a non rendere dichiarazioni (o a rendere dichiarazioni mendaci) all'autorità giudiziaria non sia diretta soltanto a ostacolare le indagini penali, ma altresì a fornire un concreto e specifico contributo al mantenimento di condotte di illegalità informatica o a danno della personalità individuale che favoriscano l'Ente.
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.6 Reati di cui all'art. 25 undecies D.Lgs. 231/01

L'art. 25 *undecies* sanziona i reati ambientali commessi nell'interesse o a vantaggio dell'Ente.
Tale disposizione potrà concorrere, nella prassi applicativa, con quella di cui all'art. 24-bis D.Lgs. n. 231/01 tutte le volte in cui fenomeni di illegalità ambientale vengano dissimulati con il ricorso a strumenti tecnologici (es., artate alterazioni dei software di rilevazione delle immissioni in atmosfera o in ambiente).
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

7.7 Reati di cui all'art. 25 quinquiesdecies D.Lgs. 231/01

L'art. 25 *quinquiesdecies* sanziona la commissione nell'interesse o a vantaggio dell'Ente dei delitti in materia tributaria di cui al D.Lgs n. 74/2000.
Tale disposizione potrà concorrere, nella prassi applicativa, con quella di cui all'art. 24-bis D.Lgs. 231/01 tutte le volte in cui la violazione di natura fiscale integrante reato avvenga nell'ambito o al fine delle condotte trattate nella presente Parte Speciale (es., artate alterazioni di documenti informatici di rilevante fiscale e contabile).
Si rimanda alla Parte Speciale specifica per i principi di comportamento e i sistemi di controllo attuati.

8. Documentazione aziendale di riferimento

- Procura al Direttore Generale;
- Organigramma;
- PIAO;
- Codice Etico;
- Policy Whistleblowing;
- Sistema Disciplinare;
- Regolamento Aziendale – *Utilizzo consapevole degli strumenti informatici*;
- Regolamenti, procedure, istruzioni e moduli interni;
- Contratto collettivo nazionale di lavoro per le lavoratrici e i lavoratori del settore gas - acqua.

L'elenco completo e aggiornato della documentazione aziendale di riferimento (compresi istruzioni, moduli e procedure interni), delle comunicazioni interne e degli ordini di servizio in vigore è disponibile presso gli uffici di competenza della sede di Cividale del Friuli.