UDINE MERCATI S.R.L.

PARTE SPECIALE
REATI INFORMATICI, VIOLAZIONI IN MATERIA DI DIRITTO D'AUTORE E IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

Modello di Organizzazione Gestione e Controllo redatto ai sensi del D.Lgs. 231 dell'8 giugno 2001 e ss.mm.ii.

Adottato dal Cda nella seduta del 28/10/2024

INDICE

1 PREMESSA

1.1 Definizioni

Nel presente documento le seguenti espressioni hanno il significato di seguito indicato:

- ***"ANAC":*** istituita con la Legge n. 190/2012, è l'autorità amministrativa indipendente la cui missione istituzionale è individuata nella prevenzione della corruzione in tutti gli ambiti dell'attività amministrativa.
- "***Attività a rischio di reato***": il processo, l'operazione, l'atto, ovvero l'insieme di operazioni e atti, che possono esporre Udine Mercati s.r.l. al rischio di sanzioni ai sensi del D.Lgs. n. 231/2001 in funzione della commissione di un Reato.
- ***"Attività Sensibili":*** attività di Udine Mercati s.r.l., individuate nel *Modello*, nel cui ambito sussiste il rischio, anche solo potenziale, di commissione dei Reati di cui al D.Lgs. n. 231/2001.
- **"*CCNL":*** Contratto Collettivo Nazionale di Lavoro per il settore del Terziario, Commercio, Distribuzione e Servizi Confcommercio sottoscritto il 22 marzo 2024 per i lavoratori dipendenti di Udine Mercati s.r.l. e sue successive modifiche, integrazioni, e rinnovi.
- **"*Cloud*": il server a cui si accede tramite Internet e il software e i database che si eseguono su quel server.
- "***Codice Etico***": il documento - previsto dall'art. 54 comma 5 del D.Lgs. n. 165/2001 (come sostituito dall'art. 1, comma 44, della Legge n. 190/2012) e dal D.P.R. n. 62/2013 (da ultimo modificato dal D.P.R. n. 81/2023), e ss.mm.ii. – approvato dal vertice di Udine Mercati s.r.l. quale esplicazione della politica societaria, che contiene i principi etici e di comportamento - ovvero, raccomandazioni, obblighi e/o divieti - a cui i Destinatari devono attenersi e la cui violazione è sanzionata.
- ***"Consulenti":*** coloro che agiscono in nome e/o per conto di Udine Mercati s.r.l. sulla base di un mandato o di altro rapporto di collaborazione.
- ***"Controllo Analogo":*** la situazione in cui una Pubblica Amministrazione esercita su una società un controllo analogo a quello esercitato sui propri servizi, esercitando un'influenza determinante sia sugli obiettivi strategici che sulle decisioni significative della società controllata. Tale controllo può anche essere esercitato da una persona giuridica diversa, a sua volta controllata allo stesso modo dall'amministrazione partecipante.
- ***"Custode dell'identità del segnalante"***: il RPCT, come qui definito.
- "***Data Protection Officer"*** o ***"DPO":*** la figura prevista dall'art. 37 del Regolamento UE 2016/679 (c.d. GDPR), designato dal Titolare (o dal responsabile) per svolgere attività consultiva, di controllo e di supporto all'applicazione del GDPR e punto di contatto con il Garante per la Protezione dei Dati Personali (c.d. GDPD).
- ***"Denuncia"***: la denuncia effettuata presso l'Autorità Giudiziaria (es. denuncia alla Procura della

Repubblica) o Contabile (Procura della Corte dei conti) ai sensi di quanto previsto dalla Legge.

- "***Destinatari***": Organi Sociali (l'Assemblea dei Soci, l'Amministratore Unico e il Consiglio di Amministrazione; l'Organo di Controllo/Sindaco Unico), Organi di Controllo (Organismo di Vigilanza, Responsabile per la Prevenzione della Corruzione e per la Trasparenza, Revisori/Società di revisione, Data Protection Officer ex GDPR, Organismi Interni di Valutazione), Personale dipendente della Società (assume rilevanza, ai fini del presente documento, la posizione di tutti i dipendenti legati alla Società da un rapporto di lavoro subordinato, indipendentemente dal contratto applicato, dalla qualifica e/o inquadramento aziendali riconosciuti: dirigenti, quadri, impiegati, lavoratori a tempo determinato, lavoratori con contratto d'inserimento, stagisti etc.), il Direttore, Fornitori (e relativi dipendenti/collaboratori) e tutti coloro che operano nell'interesse o a vantaggio di Udine Mercati s.r.l., con o senza rappresentanza, anche di fatto, e a prescindere dalla natura e dal tipo di rapporto intrattenuto con il soggetto preponente (nell'ambito di tale categoria rientrano i seguenti soggetti: (i) tutti coloro che intrattengono per la Società un rapporto di lavoro di natura non subordinata (ad es. lavoratori parasubordinati, agenti (ad es. promotori), stagisti, liberi professionisti, collaboratori a progetto, i collaboratori a qualsiasi titolo ecc.); (ii) altri soggetti che agiscono in nome e/o per conto della Società e/o cui è stata conferita procura e/o delega dal Consiglio di Amministrazione/Amministratore Unico; (iii) altri soggetti terzi che abbiano con la Società rapporti contrattuali (ad es. società di outsourcing, società interinali); (iv) i fornitori, gli outsourcer e i business partners. I Destinatari sono tenuti al rispetto del *Modello 231*.

- ***"Dipendenti":*** tutte le persone fisiche che intrattengono con la Società un rapporto di lavoro subordinato (compresi i dirigenti).
- ***"Direttore di Mercato"*** *o* ***"Direttore":*** la figura e funzione prevista dal vigente *"Regolamento del Mercato Agroalimentare all'Ingrosso di Udine"* approvato dal Comune di Udine.
- "***D.Lgs. n. 231/2001***" o "***Decreto***": il Decreto Legislativo 8 giugno 2001, n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni ed integrazioni.
- "***D.Lgs. n. 24/2023***": il Decreto Legislativo n. 24 del 10.03.2023, recante la "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" (*c.d. *"Decreto Whistleblowing* "), pubblicato in Gazzetta Ufficiale n. 63 del 15 marzo 2023, e successive modificazioni ed integrazioni.

- ***"In House Providing":*** la situazione in cui una pubblica amministrazione decide di ricorrere all'autoproduzione di beni, servizi e lavori, anziché rivolgersi al mercato rispettando procedure di evidenza pubblica.
- ***"Gestore delle segnalazioni"***: il Responsabile per la Prevenzione della Corruzione e per la Trasparenza (o "RPCT") di Udine Mercati s.r.l., quale soggetto individuato dal D.Lgs. n. 24/2023 e dalla medesima Società per la ricezione e gestione delle Segnalazioni ai sensi e per gli effetti del D.Lgs. n. 24/2023 e del *Modello 231*.
- ***"Gruppo":*** Udine Mercati s.r.l. e le società da essa controllate direttamente o indirettamente ai sensi dell'art. 2359, primo e secondo comma, del Codice civile.
- "***Linee Guida ANAC***": le Linee Guida edite dall'ANAC in materia di segnalazioni ai sensi del D.Lgs. n. 24/2023 e s.m.i. (approvate con Delibere n. 301 e 311 del 12.07.2023).
- "***Linee Guida 231***": le Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo *ex* D.Lgs. n. 231/2001, pubblicate dalle associazioni di categoria, che sono state considerate ai fini della predisposizione ed adozione del *Modello*.
- "***Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001***" o "***Modello***": il Modello di Organizzazione, Gestione e Controllo ritenuto dagli Organi Sociali idoneo a prevenire i Reati previsti dal D.Lgs. n. 231/2001 e, pertanto, adottato dalla Società, ai sensi degli articoli 6 e 7 di tale Decreto Legislativo, e relativi allegati.
- "***Modello 231"***: l'insieme organico dei documenti costituenti il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001 adottato da Udine Mercati s.r.l., segnatamente compresi il Codice Etico ed il Sistema Disciplinare, nonché la Policy Whistleblowing adottata ai sensi del D.Lgs. n. 24/2023, i regolamenti denominati "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet per la gestione degli archivi cartacei*" e "*Manuale organizzativo privacy*" (ove rilevanti ai sensi del *Modello 231*) ed il Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza adottato ai sensi della Legge n. 190/2012 e s.m.i..
- "***Organismo di Vigilanza***" o "***OdV***": l'Organismo previsto dall'art. 6 del D.Lgs. n. 231/2001, per come individuato e nominato, avente il compito di vigilare sul funzionamento e l'osservanza del *Modello*, nonché sull'aggiornamento dello stesso.
- ***"Partner"*** o ***"business partners":*** controparte contrattuale di Udine Mercati s.r.l. (quali ad es. clienti, fornitori, agenti, consulenti, operatori economici in genere ex D.Lgs. n. 36/2023, etc., siano essi persone fisiche o giuridiche) con cui essa addivenga ad una qualunque forma di collaborazione contrattualmente regolata (acquisto e cessione di beni e servizi, associazione temporanea d'impresa

- ATI, joint venture, consorzi, etc.), ove destinati a cooperare con la Società nell'ambito dei Processi Sensibili o nelle attività a rischio reato.

- ***"Parte Generale":*** sezione del Modello che ne definisce l'impianto complessivo in relazione a quanto previsto dal D.Lgs. n. 231/2001 ed alle specifiche scelte compiute dalla Società nella sua elaborazione.
- ***"Parte Speciale":*** sezione del Modello nella quale sono definiti i principi di comportamento e le regole cui attenersi nello svolgimento delle Attività Sensibili e nelle Attività a rischio in relazione a classi omogenee di fattispecie di Reato a cui la Società è, anche solo potenzialmente, esposta, nonché sistema di prevenzione ai sensi della Legge n. 190/2012 e s.m.i..
- "***Personale***": tutte le persone fisiche che intrattengono con la Società un rapporto di lavoro (inclusi il Direttore, i lavoratori dipendenti, gli interinali, i collaboratori a qualsiasi titolo, gli "*stagisti*", i volontari, i procuratori/delegati dall'Organo Amministrativo, nonché i liberi professionisti che abbiano ricevuto un incarico da parte di Udine Mercati s.r.l.).
- "***Personale Apicale***": i soggetti di cui all'articolo 5, comma 1 lett. a), del D.Lgs. n. 231/2001, ovvero i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società, ovvero che esercitano – anche di fatto – la gestione o il controllo della medesima (in particolare, il Presidente, i Vicepresidenti, i membri del Consiglio di Amministrazione, il Direttore, gli eventuali institori ed i soggetti che siano destinatari di procura e/o delega da parte dell'Organo Amministrativo della Società)[1].

- "***Personale sottoposto ad altrui direzione***": i soggetti di cui all'articolo 5, comma 1 lett. b), del D.Lgs. n. 231/2001, ovvero tutto il Personale che opera sotto la direzione o la vigilanza del Personale Apicale.

- ***"Policy Whistleblowing"***: procedura (adottata ai sensi del D.Lgs. n. 24/2023 e quale parte integrante del proprio *Modello* e del proprio *PTPCT*) che definisce in Udine Mercati s.r.l. il modello di ricevimento e di gestione delle segnalazioni interne, nonché il canale interno di segnalazione, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti anche dal trattamento di dati personali effettuatati per la gestione delle stesse, nel rispetto di quanto previsto dal Regolamento (UE) 2016/679, del D.Lgs. n. 196/2003 e del D.Lgs. n. 51/2018, e s.m.i..

- "***Pubblica Amministrazione***" o "***P.A.***": per Amministrazione Pubblica si deve intendere: (i) lo Stato (o Amministrazione Statale); (ii) gli Enti Pubblici, economici o meno: si specifica che l'Ente Pubblico è

[1] Con la sentenza n. 3211 del 16 gennaio 2024, la quinta sezione penale della Corte di Cassazione ha reso una propria interpretazione in merito alla nozione di "*esercizio di fatto della gestione e del controllo dell'ente*" e all'estensione della categoria dei soggetti apicali "*di fatto*": discostandosi da altra impostazione interpretativa che riferisce il termine "*controllo*" alla sola nozione delineata dall'art. 2359 c.c., la Corte ha adottato una soluzione interpretativa di carattere estensivo, secondo la quale la nozione di controllo ricomprende "*anche un'attività di '**controllo'** e di vigilanza o, comunque, di verifica ed incidenza nella realtà economico patrimoniale della società, **sovrapponibile a quella dei sindaci o degli altri soggetti formalmente deputati a tali attività***".

individuato come tale dalla Legge oppure è un Ente sottoposto ad un sistema di controlli pubblici, all'ingerenza dello Stato o di altra Amministrazione per ciò che concerne la nomina e la revoca dei suoi amministratori, nonché l'Amministrazione dell'Ente stesso. È caratterizzato dalla partecipazione dello Stato, o di altra Amministrazione Pubblica, alle spese di gestione; oppure dal potere di direttiva che lo Stato vanta nei confronti dei suoi organi; o dal finanziamento pubblico istituzionale; o dalla costituzione ad iniziativa pubblica); (iii) il Pubblico Ufficiale: colui che esercita "*una pubblica funzione legislativa, giudiziaria o amministrativa"* (agli effetti della legge penale "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*": art. 357 del codice penale); (iv) l'incaricato di Pubblico Servizio: colui che *"a qualunque titolo presta un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*" (art. 358 c.p.: si rappresenta che *"a qualunque titolo"* deve intendersi nel senso che un soggetto esercita una pubblica funzione, anche senza una formale o regolare investitura (incaricato di un pubblico servizio "di fatto") e non rileva il rapporto tra la P.A. e il soggetto che esplica il servizio.

- "***Protocollo"*** o ***"Procedura""***: la misura organizzativa, fisica e/o logica prevista dal *Modello* al fine di prevenire il rischio di commissione dei Reati.

- "***PTPCT":*** il Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza approvato da Udine Mercati s.r.l. ai sensi della Legge n. 190/2012 e s.m.i. e del Piano Nazionale Anticorruzione.

- "***Reati***" o il "***Reato***": l'insieme dei reati, o il singolo reato, richiamati dal D.Lgs. n. 231/2001 e dalla Legge n. 190/2012 (per come eventualmente modificati e integrati in futuro).

- "***Regolamento del Mercato Agroalimentare all'Ingrosso di Udine"*** o ***"Regolamento del Mercato":*** disposizioni regolamentari adottate dal Comune di Udine, da ultimo con Deliberazione del Consiglio Comunale n. 8 del 21.02.2022.

- "***Responsabile della funzione disciplinare***": il soggetto deputato alla gestione del procedimento disciplinare secondo quanto previsto dalla normativa e dalla prassi vigente nonché dallo Statuto e dai Regolamenti interni della Società e, comunque, dalla contrattazione collettiva applicabile. Il Responsabile della funzione disciplinare è, in ogni caso, soggetto diverso dal RPCT laddove il procedimento disciplinare scaturisca dalla segnalazione *whistleblowing.*

- ***"RPCT":*** il Responsabile della Prevenzione della Corruzione e della Trasparenza di Udine Mercati s.r.l., nominato ex art. 1, comma 7, della Legge n. 190/2012, nella rispettiva funzione di soggetto incaricato

del compito di ricevere le segnalazioni di illecito e gestirne il procedimento fino alla trasmissione della segnalazione al soggetto competente, cui competono i compiti, poteri e doveri di cui – in particolare – agli artt. 4-5-21 del D.Lgs. n. 24/2023, nonché alla Legge n. 190/2012, ai D.Lgs. nn. 33 e 39/2013[2] ed al D.P.R. n. 62/2013 e s.m.i..

- ***"Regole e Principi Generali":*** le regole ed i principi generali di cui al *Modello* specificatamente individuati.
- "***Sistema Disciplinare***": l'insieme di regole e misure sanzionatorie da applicare in caso di violazione delle regole procedimentali e comportamentali previste dal *Modello 231*.
- ***"Sistema informatico"*** o ***"telematico":*** l'insieme di apparecchiature destinate a compiere una funzione utile all'uomo attraverso il ricorso a tecnologie informatiche.
- ***"Società":*** Udine Mercati s.r.l..
- ***"Whistleblowing":*** il processo di *Segnalazione* degli illeciti che comportino *Violazioni* ai sensi del D.Lgs. n. 24/2023.

1.2 Normativa, provvedimenti e disposizioni.

La disciplina cui fa riferimento il presente documento è reperibile come segue: (i) normativa, al link: https://www.normattiva.it/; (ii) provvedimenti delle Autorità (in particolare: Autorità Nazionale Anticorruzione (ANAC), al link: https://www.anticorruzione.it/; Agenzia per l'Italia Digitale (AGID), al link: https://www.agid.gov.it/; Garante per la Protezione dei Dati Personali (GPDP), al link: https://www.garanteprivacy.it/); (iii) disposizioni interne di riferimento (fra cui: il Modello di Organizzazione Gestione e Controllo adottato dalla Società, e menzionati allegati, lo Statuto, i Regolamenti e le Procedure interne, il Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza, tutti presso la sede aziendale ed in parte al link presente sul sito aziendale www.udinemercati.com).

[2] La Corte costituzionale, con sentenza n. 98/2024, ha dichiarato l'illegittimità costituzionale degli articoli 1, comma 2, lettera f), e 7, comma 2, lettera d) del D.lgs. n. 39/2013, nella parte in cui non consentono di conferire l'incarico di amministratore di ente di diritto privato, a chi, nell'anno precedente, abbia ricoperto la carica di presidente o amministratore delegato di enti di diritto privato controllati da amministrazioni locali. In conseguenza di ciò è possibile per colui che, in provenienza, sia stato presidente o amministratore delegato di un ente di diritto privato in controllo pubblico andare a ricoprire, in destinazione, l'incarico di amministratore in un'altra società pubblica. L'intervento della Corte sul comma 2 ha lasciato in vita la analoga disposizione del comma 1, che riguarda il livello regionale.: l'ANAC – con segnalazione n. 2/2024 – ha sottoposto al legislatore, ovvero di rivedere, nel senso voluto dalla Corte, l'intero articolo «*rimuovendo, in via generale, gli incarichi di presidente o amministratore delegato di un ente di diritto privato in controllo pubblico (comma 1 ultima parte e comma 2 ultima parte dell'art. 7 del d.lgs. n. 39/2013) tra quelli che rilevano in provenienza e, in quanto tali, assumono valenza ostativa al conferimento di tutti gli incarichi in destinazione presi in considerazione dall'articolo 7 del d.lgs. n. 39/2013*».

1.3 Oggetto della presente Parte Speciale.

La presente Parte Speciale costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo di cui Udine Mercati s.r.l. (di seguito anche solo la "*Società*") si è dotata al fine di adempiere alle previsioni del D.Lgs. n. 231 del 08.06.2021 (di seguito per brevità anche il "*Decreto*"), in relazione ai reati previsti dagli **artt. 24-*bis,* 25-*octies.1* *e* 25-*novies*** del D.Lgs. n. 231/2001.

Nelle specifiche matrici di mappatura sono state rilevate le Attività Sensibili esposte a potenzialità commissive di tali reati incidenti sulla integrità della Società.

L'adozione da parte di Udine Mercati s.r.l. 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, il Direttore, i Dirigenti, i Lavoratori, i componenti degli Organi di Controllo (compreso Organismo di Vigilanza, Organismo Interno di Valutazione, Data Protection Officer, RPCT, etc.), i Collaboratori esterni a qualsiasi titolo e chiunque svolga, a qualsiasi titolo, funzioni di rappresentanza anche di mero fatto di Udine Mercati s.r.l..

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.

La responsabilità amministrativa dell'Ente, che rende possibile l'applicazione delle sanzioni previste dal D.Lgs. n. 231/2001, si fonda su una colpa "*di organizzazione*": l'Ente è ritenuto corresponsabile del reato del suo esponente se ha omesso di darsi un'organizzazione in grado di impedirne efficacemente la realizzazione e, in particolare, se ha omesso di dotarsi di un sistema di controllo interno e di adeguate procedure per lo svolgimento delle attività a maggior rischio di commissione di illeciti.

Tre sono, in sintesi, i requisiti da cui dipende la possibilità di imputare all'ente collettivo un illecito dipendente da reato: **1)** occorre che sia stato commesso da una persona fisica un certo tipo di reato (uno di quelli indicati negli artt. 24-26 del *Decreto*); **2)** occorre altresì che a commetterlo sia stata 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, infatti, è rappresentato dalla necessità che la condotta

illecita ipotizzata sia stata posta in essere dai citati soggetti *"nell'interesse o a vantaggio della Società*" e non *"nell'interesse esclusivo proprio o di terzi"* (art. 5, commi 1 e 2, del *Decreto*).

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 un'attenuazione 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, 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, infine, si accerti che un soggetto ha perseguito esclusivamente un interesse personale o di terzi, l'Ente non sarà responsabile affatto a prescindere dal vantaggio eventualmente acquisito.

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»*: 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.

Va sottolineato che l'adozione di protocolli ai sensi del D.Lgs. n. 231/2001 deve necessariamente coordinarsi anche con altri ambiti normativi cui la Società è tenuta, 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 procedimenti dell'Autorità Garante in materia di Trattamento dei Dati Personali.

L'introduzione del GDPR, diventato pienamente operativo in tutti i Paesi UE a partire dal 25 maggio 2018, si inserisce all'interno di quello che, insieme alla Direttiva 2016/680, è stato definito il *"Pacchetto europeo protezione dati*" che si propone di innovare ed ammodernare l'intera normazione sul trattamento dati e la gestione delle informazioni. Va anche ricordato, al riguardo, il D.Lgs. n. 101/2018, contenente le disposizioni

per l'adeguamento della normativa nazionale ai principi del Regolamento europeo 2016/679 che ha esplicitato anche alcuni aspetti specifici e peculiari della realtà nazionale.

Al fine di creare, quindi, un sistema organico di comportamenti, Udine Mercati s.r.l. 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 *compliant* ai dettami normativi e dispositivi in materia di Privacy.

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 di reati cosiddetti "informatici", dei quali ci si occuperà nel prosieguo della presente Parte Speciale.

Gli strumenti informatici, tuttavia e 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 (le altre Parti Speciali e la *Policy Whistleblowing* Udine Mercati s.r.l.).

Vi è, infatti, 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 di 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***[3] e, per meglio comprenderne la natura, di seguito si riporta anche il testo degli **artt. 24** e **25-*quinquies*** del D.Lgs. n. 231/2001[4]:

---

[3] Si rappresenta che, con l'art. 6-ter del Decreto Legge n. 113/2024, convertito con modificazioni dalla Legge 07.10.2024 n. 143, ha introdotto l'art. 174-sexies nella Legge n. 633/1994 (in tema di diritto d'autore: vedasi infra), il quale recita: *"Art. 174-sexies. - 1. I prestatori di servizi di accesso alla rete, i soggetti gestori di motori di ricerca e i fornitori di servizi della società dell'informazione, ivi inclusi i fornitori e gli intermediari di Virtual Private Network (VPN) o comunque di soluzioni tecniche che ostacolano l'identificazione dell'indirizzo IP di origine, gli operatori di content delivery network, i fornitori di servizi di sicurezza internet e di DNS distribuiti, che si pongono tra i visitatori di un sito e gli hosting provider che agiscono come reverse proxy server per siti web, quando vengono a conoscenza che siano in corso o che siano state compiute o tentate condotte penalmente rilevanti ai sensi della presente legge, dell'articolo 615-ter o dell'articolo 640-ter del codice penale, devono segnalare immediatamente all'autorità giudiziaria o alla polizia giudiziaria tali circostanze, fornendo tutte le informazioni disponibili.*

2. I soggetti di cui al comma 1 devono designare e notificare all'Autorità per le garanzie nelle comunicazioni un punto di contatto che consenta loro di comunicare direttamente, per via elettronica, con l'Autorità medesima ai fini dell'esecuzione della presente legge. I soggetti di cui al comma 1 che non sono stabiliti nell'Unione europea e che offrono servizi in Italia devono designare per iscritto, notificando all'Autorità il nome, l'indirizzo postale e l'indirizzo di posta elettronica, una persona fisica o giuridica che funga da rappresentante legale in Italia e consenta di comunicare direttamente, per via elettronica, con l'Autorità medesima ai fini dell'esecuzione della presente legge.

3. Fuori dei casi di concorso nel reato, le omissioni della segnalazione di cui al comma 1 e della comunicazione di cui al comma 2 sono punite con la reclusione fino ad un anno. Si applica l'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231".

[4] Con riferimento a questa Parte Speciale, il D.Lgs. 231/01 è stato modificato: dalla Legge n. 90 del 28.06.2024 per quanto riguarda l'art. 24-*bis*; dal D.L. 10/08/2023 n. 105 convertito con modificazioni con la Legge n. 137 del 9/10/2023 per quanto riguarda l'art. 24; dal D.L. 21/09/2019 n. 105 convertito con modificazioni con la Legge n.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*; dal D.Lgs. 7/7/2011, n. 121 per quanto concerne l'art. 25-*novies*.

Art. 24

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

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 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[5], 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.

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.

---

[5] 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; si veda anche il D.lgs. 4 settembre 2024, n. 138 (pubblicato nella G.U. n. 230 del 1° ottobre 2024) recante il «*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*».

Sussiste poi un nesso oggettivo fra gli strumenti ed i reati informatici e le fattispecie di cui agli **artt. 25-*octies.1*** (rubricato "*delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori"*) e **25-*novies*** (rubricato "*delitti 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 e trasferimento fraudolento di valori

1. In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:
a) per il delitto di cui all'articolo 493-ter, la sanzione pecuniaria da 300 a 800 quote;
b) per il delitto di cui all'articolo 493-quater e per il delitto di cui all'articolo 640-ter, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a 500 quote.
2. Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:
a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote;
b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.
2-bis. In relazione alla commissione del delitto di cui all'art. 512-bis del codice penale si applica la sanzione pecuniaria da 250 a 600 quote.
3. Nei casi di condanna per uno dei delitti di cui ai commi 1, 2 e 2-bis 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.

Tuttavia, prima di procedere va dato conto del fatto che in data 2 luglio 2024 è stata pubblicata in Gazzetta Ufficiale la Legge 28.06.2024 n. 90 (rubricata *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"* e nel seguito anche "*legge sulla cybersicurezza*"): la Legge, in generale, mira ad aumentate la sicurezza informatica per la difesa dai cyber-attacchi, aumentando le sanzioni previste per i c.d. "*computer crimes*". In particolare, e per ciò che in questa sede rileva, la Legge n. 90/2024 ha introdotto modifiche sostanziali e procedurali riguardanti i reati informatici[6]. La legge sulla cybersicurezza -

[6] Essa, in estrema sintesi, prevede un innalzamento delle pene, estende i confini del dolo specifico, introduce nuove circostanze aggravanti e/o vieta le attenuanti per diversi reati che siano stati commessi tramite l'utilizzo di apparecchiature informatiche al fine di ottenere indebiti vantaggi con danno altrui, o per accedere abusivamente a sistemi informatici e/o per intercettare o interrompere comunicazioni informatiche e telematiche.
Di particolare rilievo pratico è la modifica all'art. 240 c.p. che regolamenta la confisca: l'art. 16, co. 1, lett. a), della Legge n. 90/2024 dispone che "*all'articolo 240, secondo comma, numero 1-bis, dopo la parola: «635-quinquies»,* sono inserite le seguenti: *«640, secondo comma, numero 2-ter)»".*

alla luce delle modifiche apportate al reato presupposto previsto e punito dall'art. **24-*bis*** del D.Lgs. n. 231/2001 ("*Delitti informatici e trattamento illecito di dati*") - ha quindi notevoli impatti in materia di responsabilità amministrativa ai sensi del D.Lgs. n. 231/2001. Innanzitutto, il *primo comma* dell'art. 24-b*is* del D.Lgs. n. 231/2001 è stato oggetto di un generale innalzamento delle sanzioni pecuniarie inflitte all'Ente in relazione alla commissione di uno dei reati informatici ivi contemplati: previsti ora *da 500 a 700 quote*, in luogo della precedente cornice edittale *da 100 a 200 quote*. Al *comma 2* dell'articolo 24-*bis, i* riferimenti all'articolo 615-*quinquies* del codice penale ("*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*": articolo abrogato dalla Legge n. 90/2024) sono stati rimossi e sostituiti con l'art. 635-*quater.1* del codice penale (i cui contenuti sono comunque sovrapponibili, seppur inaspriti dalla previsione di due nuove circostanze aggravanti). È stato poi introdotto il nuovo *comma 1-bis* dell'articolo 24-*bis,* che punisce la nuova fattispecie di estorsione mediante reati informatici (art. 629, comma 3, del Codice penale) con la sanzione pecuniaria da *trecento a ottocento* quote e con le sanzioni interdittive previste dall'art. 9, comma 2, del D.Lgs. n. 231/2001 per una durata non inferiore ai due anni**.**

Seppur, a primo avviso, appaia improbabile la configurabilità di un delitto informatico in aziende appartenenti a settori di business distanti da quello tech/cyber, in una diversa prospettiva tale configurabilità non sembra più così remota qualora la condotta criminosa attuata tramite strumenti informatici costituisca il "*mezzo*" per la realizzazione di altri e diversi illeciti il cui rischio di commissione è statisticamente più probabile nelle realtà produttive. Si pensi ad un ipotetico caso del neoassunto Responsabile commerciale della società Alpha s.p.a., *ex* dipendente della società Beta s.r.l., il quale - nonostante gli siano stati revocati i privilegi di accesso - riesce ad accedere abusivamente ai sistemi informatici della società Beta S.r.l. e a carpire dati personali e informazioni commerciali riservate al fine di sfruttarle a vantaggio della società Alpha s.p.a.. Potrebbe ritenersi configurabile, in questo caso, un concorso tra il delitto informatico di "*Accesso abusivo ad un sistema informatico o telematico*" (615-ter c.p. e 24-bis del D.Lgs. n. 231/2001) ed uno dei delitti contro l'industria ed il commercio di cui all'art. 25-bis.1 del D.Lgs. n. 231/2001. Ancora, si rifletta su un secondo ipotetico caso: un dipendente della società Gamma s.r.l., durante l'utilizzo di un macchinario privo di "*carter di protezione*", subisce un infortunio grave e la scena è ripresa da una

Quindi, anche nel caso di truffa aggravata a norma dell'art. 640, co. 2, n. 2-ter, c.p. (anche questa, introdotta dalla normativa qui in commento), è sempre ordinata la confisca dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione di tale illecito penale, nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca del profitto o del prodotto diretti.
Da segnalare anche il nuovo art. 623-quater c.p. (rubricato "*Circostanze attenuanti*")il quale prevede: *(i)* al primo comma una diminuzione delle pene comminate per i delitti di cui agli articoli 615-ter, 615-quater, 617-quater, 617-quinquies e 617-sexies "*quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità*" *(ii)* al secondo comma una diminuzione e dalla metà a due terzi delle pene previste per i delitti di cui agli articoli 615-ter, 615-quater, 617-quater, 617-quinquies e 617-sexies laddove l'autore del reato si adoperi per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

videocamera del sistema di videosorveglianza della struttura. Il direttore di stabilimento della società, prima di attivare i soccorsi, manomette il supporto del sistema di videosorveglianza sul quale erano state memorizzate le registrazioni relative all'incidente, cancellandole, per poi installare il carter di protezione sul macchinario. La condotta così descritta potrebbe rientrare nel perimetro del reato di cui all'art. 635-quater c.p. ("*Danneggiamento di sistemi informatici o telematici*") previsto e punito dall'art. 24-*bis* del D.Lgs. n. 231/2001, in quanto commessa anche nell'interesse e a vantaggio della società Gamma S.r.l., essendo volta ad evitare sia le sanzioni per le violazioni in materia di salute e sicurezza sul lavoro, sia il probabile danno reputazionale.

In realtà, la commissione di un reato informatico coincide - il più delle volte - con il verificarsi di una violazione dei dati personali (c.d. "*data breach*") prevista dall'art. 33 del Regolamento (UE) 2016/679 in materia di protezione dei dati personali ("*GDPR*"): come noto, infatti, la violazione dei dati personali è una "*violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". Nel caso in cui si verifichi una violazione dei dati personali, il GDPR - il cui rispetto, si rammenta, è obbligatorio - impone al Titolare del trattamento di notificare la violazione al Garante per la protezione dei dati personali, ciò senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che tale violazione dei dati personali comporti un rischio per i diritti e le libertà degli interessati[7].

In termini operativi - nella costruzione e/o revisione del Modello di Organizzazione Gestione e Controllo previsto dal D.Lgs. n. 231/2001 e nello sviluppo di un sistema di compliance in materia di protezione dei dati - gli Enti sono tenute a valutare i rischi e le misure di controllo da implementare per contenere le minacce informatiche in un'ottica *risk-based approach*. Nel dettaglio, è fondamentale: **(i)** stabilire ed applicare procedure interne per assicurare la sicurezza dei sistemi informatici prevedendo, ad esempio, rigide misure di segregazione degli accessi logici, al fine di impedire a soggetti non autorizzati di accedere e manomettere (come nell'esempio della società Gamma s.r.l.) strumentazione informatica; **(ii)** implementare sistemi di monitoraggio continuo per identificare tempestivamente eventuali minacce o violazioni; **(iii)** organizzare programmi di formazione per sensibilizzare i dipendenti in materia di responsabilità amministrativa degli enti con l'intento di evitare (come visto nell'esempio della società Alpha s.p.a.) che l'azione illecita di un dipendente comporti l'apertura di un procedimento ai sensi del D.Lgs. n. 231/2001 a carico dell'Ente.

[7] Va ricordato anche il D.Lgs n. 138 del 04.09.2024 in vigore dal 18.10.2024 (pubblicato sulla Gazzetta Ufficiale n. 230 del 1° ottobre 2024) di recepimento della direttiva (UE) 2022/2555 – la *Direttiva NIS2* – relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. Stabilendo misure volte ad assicurare un livello elevato di sicurezza informatica in ambito nazionale, il decreto contribuisce ad incrementare il livello comune di sicurezza nell'Unione europea così da migliorare il funzionamento del mercato interno.

2.1 Reati propriamente informatici citati dall'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* del D.Lgs. n. 231/2001 in relazione ai delitti informatici ed al trattamento illecito dei dati.

Art. 615-*ter* c.p.
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 fino a tre 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 da ultimo modificata con la citata Legge n. 90/2024. Essa si configura come un delitto comune, dato che è possibile la sua commissione da parte di "*chiunque*", ed è considerato quale reato "*istantaneo*" poiché la sua consumazione avviene nel momento dell'introduzione o nella protrazione all'interno del sistema nonostante il dissenso del titolare dello *ius excludendi*.

La fattispecie incrimina due differenti condotte: **(i)** l'introduzione abusiva in un sistema protetto; **(ii)** 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[8], 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 possono anche

[8] 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.

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.

In relazione a tale 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[9]. È configurabile il reato in commento, anche l'aver preso visione di dati per semplice curiosità, non essendo affatto 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 che integrano il reato di cui all'art. 615-*ter* c.p.: 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* c.p.
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 con la reclusione sino a due anni e con la multa sino a euro 5.164.
La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 -ter , secondo comma, numero 1).
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.

[9] 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.

Per comprendere questo reato[10], è necessario precisare 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.

Il bene giuridico oggetto di tutela della norma in commento è la c.d. riservatezza informatica e la conseguente indisturbata fruizione del sistema informatico da parte del gestore.

La norma punisce una condotta prodromica alla commissione del delitto di cui all'articolo 615-ter c.p., sanzionando la detenzione/produzione/riproduzione/diffusione/importazione/comunicazione/consegna o comunque la messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela del domicilio informatico altrui [11]. Per sistema informatico o telematico deve intendersi l'insieme di apparecchiature destinate a compiere una funzione utile all'uomo attraverso il ricorso a tecnologie informatiche.

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 rende applicabile la previsione anche a fattispecie al momento non prevedibili.

Il reato previsto dalla norma è un reato comune, di pericolo (non richiede che l'evento lesivo si realizzi effettivamente) ed istantaneo: esso richiede, come elemento soggettivo, il dolo specifico, ossia il fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

Potrebbe integrare il reato in commento:

- la condotta di chi riceve i codici di carte di credito abusivamente scaricati dal sistema informatico, ad opera di terzi, e li inserisce/associa in carte di credito clonate poi utilizzate per il prelievo di denaro contante attraverso il sistema bancomat;
- la condotta di colui che si procura abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (c.d. clonazione) è possibile realizzare una illecita connessione alla rete di

[10] modificato dalla citata Legge n. 90/2024.

[11] Si veda la Cassazione penale, sez. V, nella sentenza n. 21987/2019 secondo cui: "*Il domicilio informatico è da intendere, in linea con quanto emergente dalla Raccomandazione del Consiglio d'Europa del 9.9.1989, "quale spazio ideale di esclusiva pertinenza di una persona fisica o giuridica, delimitabile prendendo come parametro il domicilio delle persone fisiche, ed al quale risulta estensibile la tutela della riservatezza della sfera individuale, che costituisce bene costituzionalmente protetto"*. Sempre la Corte di Cassazione, sez. V Penale, nella sentenza n. 27900/2023 quanto alla qualificazione di domicilio informatico al "*cloud*" (il server a cui si accede tramite Internet e il software e i database che si eseguono su quel server).

telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche.

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

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da 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.

Anche il reato di cui all'art. 617 quater c.p. è stato oggetto di modifica ad opera della L. 90/2024.
La norma in esame è posta a tutela della inviolabilità delle comunicazioni a distanza tra due o più soggetti.
L'oggetto della condotta prevista dal primo comma è rappresentato dall'apprendere in maniera fraudolenta comunicazioni relative ad un sistema informatico o tra sistemi telematici, ovvero interromperle o impedirle.
La fraudolenza della condotta qualifica il mezzo usato per prendere cognizione della comunicazione, con la conseguenza che lo strumento utilizzato deve caratterizzarsi per la sua idoneità ad eludere la possibilità di percezione della captazione da parte dei soggetti tra i quali intercorre la comunicazione.
Il secondo comma, invece, prevede la medesima pena nei confronti di chi riveli pubblicamente il contenuto delle comunicazioni captate fraudolentemente da altri.
Il comma 4 prevede alcune circostanze aggravanti specifiche.
Esempi di condotte sanzionate: 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 c.p.
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 (modificato dapprima dall'art. 19 della Legge n. 238/2021 e, quindi da ultimo, dalla Legge n. 90/2024) è parimenti relativo alla riservatezza e della libertà e segretezza delle comunicazioni a distanza tra due o più soggetti: per effetto della ultima riforma è stato ampliato il novero delle condotte punibili.
La norma in commento punisce fatti prodromici alla commissione del delitto di cui all'articolo precedente 617 quater c.p., indicando come penalmente rilevante di chi procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a captare/intercettare o impedire comunicazioni relative ad un sistema informatico o tra sistemi telematici (primo comma).

Il secondo comma, invece, prevede una circostanza aggravante specifica, qualora il fatto sia commesso in danno di un sistema informatico dello Stato, oppure sia commesso da un pubblico ufficiale con abuso dei poteri o con abuso della qualità di operatore del sistema, o se commesso da chi eserciti, anche abusivamente, la professione di investigatore privato.
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.
Ad esempio, può configurare il reato in esame, la condotta di colui che installi, all'interno del sistema bancomat di un'agenzia di banca, uno scanner per bande magnetiche con batteria autonoma di alimentazione e microchip per la raccolta e la memorizzazione dei dati, al fine di intercettare comunicazioni relative al sistema informatico.

Art. 629 c.p.
Estorsione

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.

Per quanto d'interesse in relazione al D.Lgs. n. 231/2001, viene preso in considerazione solo il terzo comma, introdotto dall'art. 16 comma 1, lett. m), n. 2) della Legge n. 90/2024.

Il citato comma punisce (severamente) la c.d. "*estorsione informatica*". La fattispecie mira a contrastare il fenomeno dei "*ramsoware*"[12], ovvero dei virus che bloccano l'accesso ai file dell'utente richiedendo una somma di denaro in cambio, solitamente in cripto valute. La fattispecie è "a condotta complessa" e consiste in due fasi, ovvero la commissione di uno dei reati "informatici" citati nella norma (acceso abusivo a sistema informatico, intercettazione informatica abusiva, ecc..) o "la minaccia di compierli" costringendo taluno a fare od omettere qualcosa nonché procurando a sé un profitto "ingiusto".

Si può trattare, per esempio, di divulgazione di informazioni sensibili dei dipendenti di un'azienda o dei suoi clienti ovvero di dati confidenziali che, se divulgati, potrebbero danneggiare la reputazione di un soggetto o di un'azienda.

Art. 635 bis c.p.
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[13] ricalca quanto 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. Non è richiesto il dolo specifico e sono sanzionati comportamenti ed omissioni sia di chi agisce volendo esplicitamente e ricercando il danneggiamento, sia quella di chi è consapevole che il suo comportamento potrebbe comportare un danneggiamento ma confida nella sorte.

È un reato di evento e, ai sensi dell'art. 56 c.p., si può ritenere configurabile il tentativo laddove la condotta non pervenga a determinare la distruzione, alterazione o deteriorazione di dati o programmi informatici. È un reato sottoposto a condizione di procedibilità (querela della persona offesa) e come tale non perseguibile d'ufficio. Come già anticipato, essendo sottoposti a tutela i dati ed i programmi informatici altrui, è inequivocabile come il bene giuridico meritevole di tutela sia il patrimonio.

---

[12] Può dirsi che allo stato si definiscono sono due tipi di ransomware: *"cryptor"* che, con un algoritmo la cui chiave è conosciuta ai soli programmatori, crittografa i file contenuti nella macchina bersaglio rendendoli non più accessibili; "*blocker",* che, più semplicemente, impediscono l'accesso al dispositivo bersaglio In entrambi i casi, il malware mostra una finestra pop-up in cui vengono riportate le istruzioni per ottenere la chiave di cifratura per lo sblocco dei file o della macchina dietro il pagamento di una somma di danaro, ma questa soluzione non sempre garantisce lo sblocco: in ogni caso, rappresenta un odioso attacco ai beni immateriali della persona offesa (i dati) a cui il legislatore ha deciso di porre un freno. Altre condotte estorsive possono concretizzarsi nella minaccia di informare le autorità del data breach (es. Garante Privacy), di diffondere i dati o di offrirli in vendita sul deep web.

[13] Anch'esso modificato dalla citata Legge n. 90/2024, con notevole inasprimento delle pene edittali e la previsione di aggravanti ad effetto speciale. Vedasi anche nota 20.

È un reato comune, non qualificato, proprio perché può essere commesso da chiunque (salvo la circostanza aggravante di cui al comma 2 che incrimina la condotta dell'operatore informatico o di chi impieghi violenza o minaccia alla persona). Ulteriore condizione è, ovviamente, che i dati e programmi informatici siano "altrui".

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 c.p.
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[14] costituisce un'ipotesi autonoma di reato (non, quindi, un'ipotesi aggravata di quanto previsto dall'art. 635 bis c.p.: infatti, la norma in esame punisce anche condotte prodromiche al danneggiamento di dati o programmi informatici in uso ad un organo statale).

Il bene giuridico tutelato è il patrimonio, in relazione ai dati ed ai programmi informatici statali.

La disposizione, al primo comma, ricalca essenzialmente lo schema del tentativo di reato ("un fatto diretto a…" - art. 56 c.p.). Se invece il danneggiamento o gli altri eventi di danno si realizzano, la pena è aumentata.

Esso si qualifica quale reato comune (pertanto, può essere commesso da chiunque) e 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 c.p.
Danneggiamento di sistemi informatici o telematici

[14] Articolo inserito dalla Legge n. 48/2008 e, come l'art. 635 bis c.p., oggetto di modifica da ultimo dalla Legge n. 90/2024 (anche qui con inasprimento delle pene e la previsione di aggravanti ad effetto speciale). Vedasi anche nota 20.

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. 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.

Rispetto al dettato normativo di cui all'art. 635 bis c.p., questo articolo[15] sanziona ulteriori condotte criminose, ossia il danneggiare od ostacolare il funzionamento del sistema informatico o telematico *"altrui*", non solo mediante distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui (art. 635 bis c.p.), ma anche "*attraverso l'introduzione o la trasmissione di dati, informazioni o programmi"*.

In altri termini: ad essere incriminata è la condotta di chi, tramite la distruzione, la cancellazione, il deterioramento o alterazione di dati o programmi informatici, o mediante l'introduzione abusiva nel sistema informatico, distrugge, cancella, deteriora o altera sistemi informatici o telematici altrui.

È previsto un aggravamento di pena, ai sensi del secondo comma, se il fatto è commesso con violenza o minaccia, oppure abusando della propria qualità di operatore informatico.

Art. 635 quater.1 c.p.
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.

L'articolo in commento (inserito dall'art. 16, comma 1, lett. q), L. 28 giugno 2024, n. 90, a decorrere dal 17 luglio 2024) è volto 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

[15] Articolo inserito dalla Legge n. 48/2008 ed oggetto di modifica da ultima ad opera della Legge n. 90/2024 (che ha aggravato le pene edittali e previsto aggravanti ad effetto speciale).

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: è punito chi diffonde, comunica o consegna un programma informatico (sia frutto del proprio ingegno, che di altri):

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

Affinché si possa configurare il reato in esame è irrilevante che il fine ultimo sia quello di procurare un danno od un'interruzione parziale.

Trattasi di reato comune, che 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 c.p.
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).

L'articolo in commento[16] costituisce un'ipotesi autonoma di reato (e non un'ipotesi aggravata dell'art. 635-*quate*r c.p.: infatti, la norma in esame punisce anche condotte prodromiche al danneggiamento di un sistema informatico di pubblica utilità).

Il bene giuridico tutelato è il patrimonio, in relazione ai sistemi informatici di pubblica utilità.

[16] Originariamente inserito dalla Legge n. 48/2008 e integralmente sostituito dalla Legge n. 90/2024. Vedasi anche nota 20.

La disposizione di cui al primo comma ricalca essenzialmente lo schema del tentativo di reato di cui all'art. 56 c.p. (*"compie atti diretti a…"*). Se invece il danneggiamento o gli altri eventi di danno si realizzano, la pena è aumentata.

Se il fatto è commesso con violenza o minaccia, oppure abusando della propria qualità di operatore informatico, si applica un aggravamento di pena ai sensi del secondo comma.

Essendo un reato di pericolo, ai fini della sua configurazione non è richiesto che si produca il danneggiamento dei sistemi informatici e telematici di pubblica utilità, ovvero che ne sia effettivamente ostacolato il funzionamento[17].

2.2 Falsità e frode informatica ed illeciti negli approvvigionamenti di beni e servizi

Mentre gli articoli indicati nei **commi 1) – 1 bis) – 2)** 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 aspetti relativi agli incanti (art. 353 del codice penale);
- la turbata libertà del procedimento di scelta del contraente (art. 353-bis del c.p.);
- la frode nelle pubbliche forniture (art. 356 del c.p.);
- il reato di Frode Informatica (art. 640-ter del c.p.).

Tali reati presupposto verranno esposti (anche) in questa Parte Speciale, in ragione altresì dell'emanazione del Codice degli Appalti di cui al D.Lgs. n. 36/2023, che prevede – fra le altre - la creazione di un ecosistema digitale quale strumento per la digitalizzazione del ciclo di vita dei contratti e la piena effettività dell'*eProcurement*[18] (*cfr*. in particolare art. 22 del D.Lgs. n. 36/2023).

Art. 491 bis c.p.
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.

[17] Si ricorda che, 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 allorché "*il fatto risulti di lieve entità*".

[18] 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.

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) . Dunque, con la locuzione "*documento informatico*"[19] ci si riferisce al *"documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*. 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[20].

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

Figura 1 – Varie tipologie di firma

[19] 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"* e s.m.i..

[20] 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".*

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 c.p.
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[21] riconducibili all'articolo in esame sono le seguenti:

[21] La struttura del reato di cui all'art. 640 *ter* è duplice: da un lato, infatti, si persegue la ipotesi di chi "alteri", in qualsiasi modo, il funzionamento di un sistema informatico o telematico, intendendosi, per "alterazione" un intervento modificativo o manipolativo sul funzionamento del sistema che viene "distratto" dai suoi schemi predefiniti, in vista del raggiungimento dell'obiettivo, punito dalla norma, di conseguire per sé o per altri un in-giusto profitto con altrui danno. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato, il che consente di differenziare la frode informatica dai delitti di danneggiamento informatico (artt. 635 bis, ter, quater, quinquies c.p.) non solo perché in questi ultimi è assente ogni riferimento all'ingiusto profitto, ma anche perché l'elemento materiale dei suddetti reati è costituito dal mero danneggiamento dei sistemi informatici o telematici, e quindi da una condotta finalizzata a impedire che il sistema funzioni o perché il medesimo è reso inservibile (attraverso la distruzione o danneggia-mento), o perché se ne ostacola gravemente il funzionamento. L'altra ipotesi descritta dalla norma è costituita invece dalla condotta di chi intervenga "senza diritto" con qualsiasi modalità, su "dati, informazioni o programmi" contenuti nel sistema, così da realizzare, anche in questo caso, l'ingiusto profitto con correlativo altrui danno: in questa ipotesi, dunque, attraverso una condotta a forma libera, si "penetra" abusivamente all'interno del sistema, e si opera su dati, informazioni o programmi, senza che il sistema stesso risulti in sé alterato. Il bene giuridico tutelato dal delitto di frode informatica non può, dunque, essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, venendo chiaramente in discussione anche l'esigenza di tutelare la regolarità di funzionamento dei sistemi informatici, sempre più capillarmente presenti in tutti i settori più importanti della vita economica, sociale ed istituzionale del Paese, oltre che la riservatezza dei dati, spesso sensibili, ivi gestiti, e infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici. In ordine al rapporto con il reato di truffa, la giurisprudenza di legittimità è concorde nel ritenere che, pur essendo comuni gli elementi costitutivi, il reato di frode informatica si differenzia dal reato di truffa, perché l'attività fraudolenta dell'agente investe non una persona, quale soggetto passivo della stessa, di cui difetta l'induzione in errore, ma il sistema informati-co di pertinenza della medesima, attraverso la manipolazione di tale sistema; il fatto poi che la manipolazione del sistema informatico alla fine possa determinare il compimento di un atto di disposizione patrimoniale da parte di una persona fisica non vale a cambiare la natura del reato di frode informatica, consistendo la differenza rispetto al reato di truffa nel fatto che l'atto di disposizione patrimoniale, nell'ipotesi ex art. 640 *ter* c.p., consegue alle manipolazioni informatiche anziché a una diretta induzione in errore della vittima. In applicazione di tali coordinate ermeneutiche, è stata ricompresa nell'alveo della previsione criminosa di cui all'art. 640 *ter* c.p. la condotta illecita di chi, entrato senza diritto in possesso delle cifre chiave e delle password di altre persone, utilizzi contra ius tali elementi per accedere ai sistemi informatici bancari al fine di operare sui relativi dati contabili e disporre bonifici, accrediti o altri ordini, così procurandosi un ingiusto profitto con pari danno per i titolari dei conti oggetto degli interventi di "storno", mentre invece viene pacificamente sussunta nell'ambito del reato di truffa la vendita on line di beni il cui prezzo viene corrisposto mediante la ricarica della carta *postepay* dell'agente senza consegna della merce, investendo in tal caso l'azione fraudolenta non il sistema informatico in sé, semplice veicolo della condotta truffaldina, ma direttamente la persona offesa.
La Corte di Cassazione, con la sentenza n. 38027/2023, pronunciandosi nell'ambito di un procedimento penale per il reato di frode informatica, ha chiarito che la nozione di "identità digitale", prevista dalla circostanza aggravante di cui all'art. 640-ter, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati. Sulla base di tale principio, la Suprema Corte ha ritenuto integrata nel caso di specie la predetta aggravante, con la conseguente procedibilità d'ufficio del reato, avendo l'imputato utilizzato abusivamente i codici di accesso personale alla carta di credito, esplicitamente associata al conto corrente della persona offesa, e così realizzato un'evidente e indebita sostituzione del titolare nella sua identità digitale collegata all'utilizzo del mezzo informatico nello svolgimento dei rapporti bancari e creditizi.

- 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. 231/2001.

Art. 640 quinquies c.p.
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 quale quello delle firme elettroniche o sottoscrizioni digitali, le quali - a seconda di requisiti e caratteristiche - la legge equipara, a seconda dei casi (e senza ambire, in questa sede, a pretese di esaustività), 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 c.p.
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 euro 103 a euro 1.032.
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 euro 516 a euro 2.065.
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 c.p.
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 c.p.
Frode nelle pubbliche forniture

Chiunque commette frode nell'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 euro 1.032.
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.

Il sistema nazionale di approvvigionamento digitale[22] – 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*")[23].

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*")[24] 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.

[22] 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".

[23] https://dati.anticorruzione.it/superset/dashboard/appalti/?native_filters_key=nQ8n_sMV8P_8oK28njCN2dNf8WgK59ESKl5ns-Gw8kTNJkJeEH5hjWBATUjxpyU_

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

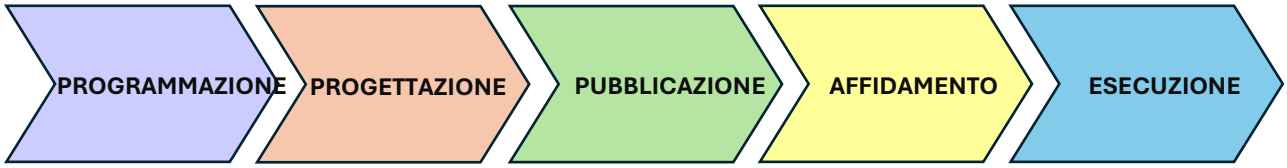

Figura 2 – Fasi del ciclo di vita dei contratti

Per meglio comprendere i contenuti di ogni fase del processo, si richiama la delibera ANAC n. 261/2023[25] che riporta, all'articolo 10[26], le informazioni che ciascuna stazione appaltante deve trasmettere per ogni fase, individuando così le attività riconducibili a ciascuna fase.

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[27], 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.

---

[25] 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.

[26] *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** 1. gli avvisi di aggiudicazione ovvero i dati di aggiudicazione per gli affidamenti non soggetti a pubblicità 2. 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.

[27] "*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".*

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 adottato dalla Commissione Europea e pubblicato l'Artificial Intelligence Act[28], che regola le modalità di utilizzo dell'intelligenza artificiale anche nelle applicazioni alla vita reale.

2.3 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 c.p.
Prostituzione minorile

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.

[28] L'AI Act è approdato in Gazzetta Ufficiale europea con il Regolamento n. 1689 del 13 giugno 2024 ed entrerà in vigore venti giorni dopo la pubblicazione in GU UE avvenuta in data 12 luglio 2024. La sua piena applicazione è prevista dal 2 agosto 2026.

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 c.p.
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 c.p.
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.
3. Fuori dei casi di cui al primo comma, chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a due anni e con la multa non inferiore a euro 1.000.

Nel reato in commento ad essere punito è chi rappresenta il "consumatore finale", e ciò non per aver cercato di far circolare materiale pornografico che coinvolge minori ma per la semplice detenzione.
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. 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 c.p.
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 ed è diretto a sanzionare la perversione dell'agente, prescindendo da una lesione effettiva del bene tutelato.

Un esempio di condotta penalmente rilevante è quella di un soggetto che detiene una pluralità di immagini e video di carattere pedopornografico virtuale (ottenuti, del resto, mediante file sharing) che si sostanzia in scene stilizzate e disegnate come cartoni animati, ma elaborate a tal punto da apparire vere, anche se non reali.

2.4 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 è stato emanato il D.Lgs n. 184/2021[29], entrato in vigore in data 14.12.2021, che ha introdotto l'art. **25-*octies.1*** nel D.Lgs. n. 231/2001 (rubricato "*delitti in materia di strumenti di pagamento diversi dai contanti*"), così estendendo 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. n. 184/2021 ha introdotto definizioni anche rispetto al Codice penale, le quali devono essere tenute in considerazione ai fini dell'interpretazione delle fattispecie[30].

In sintesi, i reati presupposto intendono reprimere e censurare 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;
- il possesso, la cessione o l'acquisizione di strumenti di pagamento di provenienza illecita, falsificati o alterati;
- la produzione, importazione, esportazione, vendita, trasporto, distribuzione, mettere a disposizione o in qualsiasi modo procurare a sé o a altri apparecchiature, dispositivi o programmi informatici che permettono la commissione dei reati riguardanti strumenti di pagamento diversi dai contanti;

[29] 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*".

[30] *<<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>>.

- trasferimento di denaro, di valore monetario o di valuta virtuale mediante frode informatica.

L'art. 25-*octies.1* è stato poi oggetto di modifica ad opera del D.L. n. 10 agosto 2023 n. 105, convertito, con modificazioni, dalla L. 9 ottobre 2023 n. 137.

Di seguito, si riportano i disposti normativi sopra richiamati e contenuti nell'art. 25-*octies.1* del D.Lgs. n. 231/2001:

Art. 493-ter c.p.
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.

In tale articolo[31] sono indicate tre distinte condotte criminose, punite in egual modo: **(i)** 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); **(ii)** chi, sempre al fine di trarne profitto, falsifica tali strumenti di pagamento; **(ii)** chi 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, richiesto l'effettivo conseguimento di un profitto, purché venga accertato il dolo specifico.

Art. 493-quater c.p.
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

[31] Articolo inserito dall'art. 4, comma 1 lett. a), del D.Lgs n. 21/2018 e poi modificato dall'art. 2 del D.Lgs n. 84/2021, a decorrere dal 14 dicembre 2021.

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.

Rispetto all'art. 493-ter c.p., la fattispecie[32] in commento 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 c.p.
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.

Ai sensi del D.Lgs. n. 231/2001 viene preso in considerazione il secondo comma dell'art. 640-ter c.p. (modificato dall'art. 2, comma 1, lett. c) del citato D.Lgs n. 184/2021, a decorrere dal 14 dicembre 2021).
Con il reato in commento, il Legislatore ha inteso punire il caso in cui la frode informatica produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

Art. 25-octies.1, secondo comma D.Lgs. 231/01
Altre fattispecie

[32] Articolo inserito dall'art. 2, comma 1, lett. b), del D.Lgs 184/2021, a decorrere dal 14 dicembre 2021.

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

Il secondo comma dell'art. 25-*octies.1* del D.Lgs. n. 231/2001 contiene una norma di chiusura che stabilisce la punibilità dell'Ente anche 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, salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente.

Tale previsione normativa sembra, però, introdurre una significativa eccezione al principio del "numero chiuso" dei reati presupposto contenuti nel D.L.gs. n. 231/2001, poiché una interpretazione rigorosa della stessa potrebbe portare alla configurabilità della suddetta responsabilità in relazione a reati che non rientrano tra quelli presupposto e costringerebbe così gli Enti ad un'attività di *compliance* potenzialmente estesa a qualsiasi fattispecie di reato.

Art. 512 bis c.p.
Trasferimento fraudolento di valori

Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter, è punito con la reclusione da due a sei anni.
La stessa pena di cui al primo comma si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

L'articolo in commento è stato inserito dal D.L.gs. 1° marzo 2018 n. 21, mentre il secondo comma è stato di recente inserito mediante il D.L. 2 marzo 2024, n. 19, convertito nella Legge 29 aprile 2024, n. 56.

Il primo comma punisce l'attribuzione fittizia della titolarità o della disponibilità di beni al fine di eludere le misure di prevenzione patrimoniale o di agevolare la commissione dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita. Si presenta, quindi, come una fattispecie ad ampio raggio, dove la condotta – fraudolenta, a forma libera e sorretta dal dolo specifico – risulta svincolata da un contesto di azione determinato e ha come oggetto denaro, beni o altre utilità ovvero i beni e i rapporti patrimoniali di cui può essere titolare il proposto alla prevenzione patrimoniale e possono ricadere nello spettro del sequestro e della confisca *ex* D.Lgs. n. 159/2011 oppure essere l'oggetto dei reati menzionati.

Di conseguenza, queste misure divengono l'oggetto del dolo specifico, che selezionano l'ambito di applicabilità dell'incriminazione.

Il disposto del secondo comma si pone in un rapporto di specialità rispetto alla previsione del comma 1.

Tali profili di specialità riguardano l'oggetto della condotta e il contesto in cui viene posta in essere, circostanza che pare costituire una condizione obiettiva di punibilità: infatti, la condotta elusiva ha come oggetto le disposizioni di documentazione antimafia ovvero – *ex* art. 84 D.L.gs. n. 159/2011 – la comunicazione antimafia e l'informazione antimafia e, quindi, le certificazioni poste a base di tali provvedimenti amministrativi, che nell'economia del nuovo Codice degli Codice dei Contratti Pubblici (D.Lgs. n. 36/2023) sono requisiti essenziali perché un operatore economico possa partecipare ad una gara pubblica ed eseguire la prestazione appaltata.

Pertanto, anche il profilo soggettivo risulta diverso da quello del comma 1: sebbene la norma lo costruisca come un reato comune, nei fatti si tratta di un delitto a soggettività ristretta. La documentazione antimafia, infatti, ex art. 85 D.Lgs. n. 152/2011, è richiesta – nel caso di imprese individuali – al titolare e al direttore tecnico, mentre – nel caso di Enti – al direttore tecnico, al legale rappresentante, ai componenti dell'organo amministrativo e via continuando, ossia a chi esercita un'attività d'impresa in vari ruoli.

Così, anche l'oggetto della condotta viene ridescritto in funzione della documentazione antimafia, individuandolo nella: **i)** titolarità dell'impresa; **ii)** nell'appartenenza delle quote sociali e **iii)** nelle persone che rivestono le cariche sociali ovvero l'oggetto di valutazione della comunicazione e dell'informazione antimafia.

Possono rientrare nella sfera di punibilità prevista dalla disposizione, ad esempio, la nomina fittizia di un prestanome come amministratore di una società, al quale sia attribuita la titolarità del conto corrente bancario della società, con potere di disporre delle risorse della medesima, ovvero, la costituzione di una nuova attività d'impresa esercitata in forma societaria con la medesima finalità richiamata dalla norma.

2.5 Delitti in materia di violazione del diritto d'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 i seguenti disposti normativi della Legge n. 633/1941[33]:

- 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;

[33] Vedasi nota 3.

- 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.

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.

La previsione dell'art. 171 rileva ai fini del D.Lgs n. 231/2001 solo con riguardo al testo sopra riportato ed opera sempre fatto salvo quanto previsto dalle specifiche previsioni dei successivi articoli 171-*bis* e 171-*ter.*
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.

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.

Le norma dell'art. 171-*bis* [34] vede come bene giuridico tutelato 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, in particolare, il reato di cui all'art. 171-*bis* 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;

[34] Introdotto dal D.Lgs. n. 518/1992, che ha provveduto ad estendere la tutela del Diritto d'Autore ai programmi per elaboratore, e poi oggetto di modifiche con il D.Lgs. n. 169/1999, che ha ulteriormente ampliato l'ambito di tutela alle banche dati e, quindi, con la Legge n. 248/2000 e con la Legge 43/2005 di conversione de DL 7/2005)

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.
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 norma[35] è di fatto volta 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.

I comportamenti censurati e colpiti dalla norma sono descritti oggettivamente ed in maniera articolata ma richiedono, per la loro sussistenza, che il fatto non sia commesso per uso personale e che l'agente persegua una finalità di lucro. Pertanto, non sono reati ricompresi 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, pertanto, la semplice rimozione delle protezioni o l'alterazione delle informazioni elettroniche relative ai diritti d'autore (ex art. 102-*quinquies)* costituiscono un reato 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 rientranti nell'ambito dell'articolo in esame sono: 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.

[35] Inserita dal D.Lgs. n. 685/1994 e successivamente modificata, da ultimo con la Legge n. 93/2023.

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, 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. In realtà vi è 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).

3 SANZIONI

Richiamato quanto indicato nella Parte Generale rispetto alle sanzioni previste dalla Sezione II del D.Lgs n. 231/2001, gli articoli **24-*bis*** e **25-*quinquies*** del D.Lgs. n. 231/2001, prevedono sanzioni **pecuniarie** applicabili all'Ente in caso di commissione dei reati ivi previsti, come da tabella che segue.

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
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 quanto agli articoli **24-*octies.1*** e **25-*novies*** del D.Lgs. n. 231/2001.

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-quater
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-octies.1 c. 2 bis (da 250 a 600 quote)	**Art. C.P.**
Trasferimento fraudolento di valori	512 bis c.p.
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

Oltre alle sanzioni pecuniarie, l'art. 9 del D.Lgs. n. 231/2001 prevede anche le **sanzioni interdittive e accessorie**, riportate nella tabella che segue.

		SANZIONE / Fonte	***Art. 24 bis***			***Art. 25 octies.1***		***Art. 25 novies***
			c.1	***c.2***	***c.3***	***c.1, c. 2 c. 2 bis***		***c.1***
		interdittive						
	Art. 9 c.2	*a) interdizione*	X			X		X (<1 anno)
		b) sospensione o revoca autorizzazioni licenze	X	X		X		X (<1 anno)
		c) divieto di contrattare con la P.A.			X	X		X (<1 anno)
		d) esclusione o revoca agevolaz. ed incentivi			X	X		X (<1 anno)
		e) divieto di pubblicizzare beni/servizi	X	X	X	X		X (<1 anno)
		c) confisca	X	X	X	X		X
		d) pubblicazione della sentenza	possibile se interd.	possibile se interd.	possibile se interd.	possibile se interd.		possibile se interd.

4 ESCLUSIONE DELLA RESPONSABILITA' AMMINISTRATIVA: GENERALITA'

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, Gestione e Controllo 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, Gestione e Controllo;

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. 231/2001) 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, Gestione e Controllo pienamente esimente, anche se il D.Lgs. n. 231/2001 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;
5) introdurre un *sistema disciplinare* idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

5 ATTIVITA' SENSIBILI AI SENSI DEL D.LGS. 231/2001. SOGGETTI COINVOLTI E DESTINATARI DELLA PRESENTE PARTE SPECIALE

Si designano come **"*attività sensibili*"** specifiche aree di attività di Udine Mercati s.r.l. 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.

6 ATTIVITA' SENSIBILI PER LA COMMISSIONE DI UNO DEI REATI PREVISTI DALL'ART. 24-BIS DEL D.LGS 231/01

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 della documentazione e della corrispondenza con privati, aziende ed Enti pubblici ed Autorità in genere.

In particolare, si sono considerati anche i processi di *eProcurement* svolti effettivamente all'interno di Udine Mercati s.r.l. e si è proceduto ad una loro mappatura, che viene presentata in figura seguente.

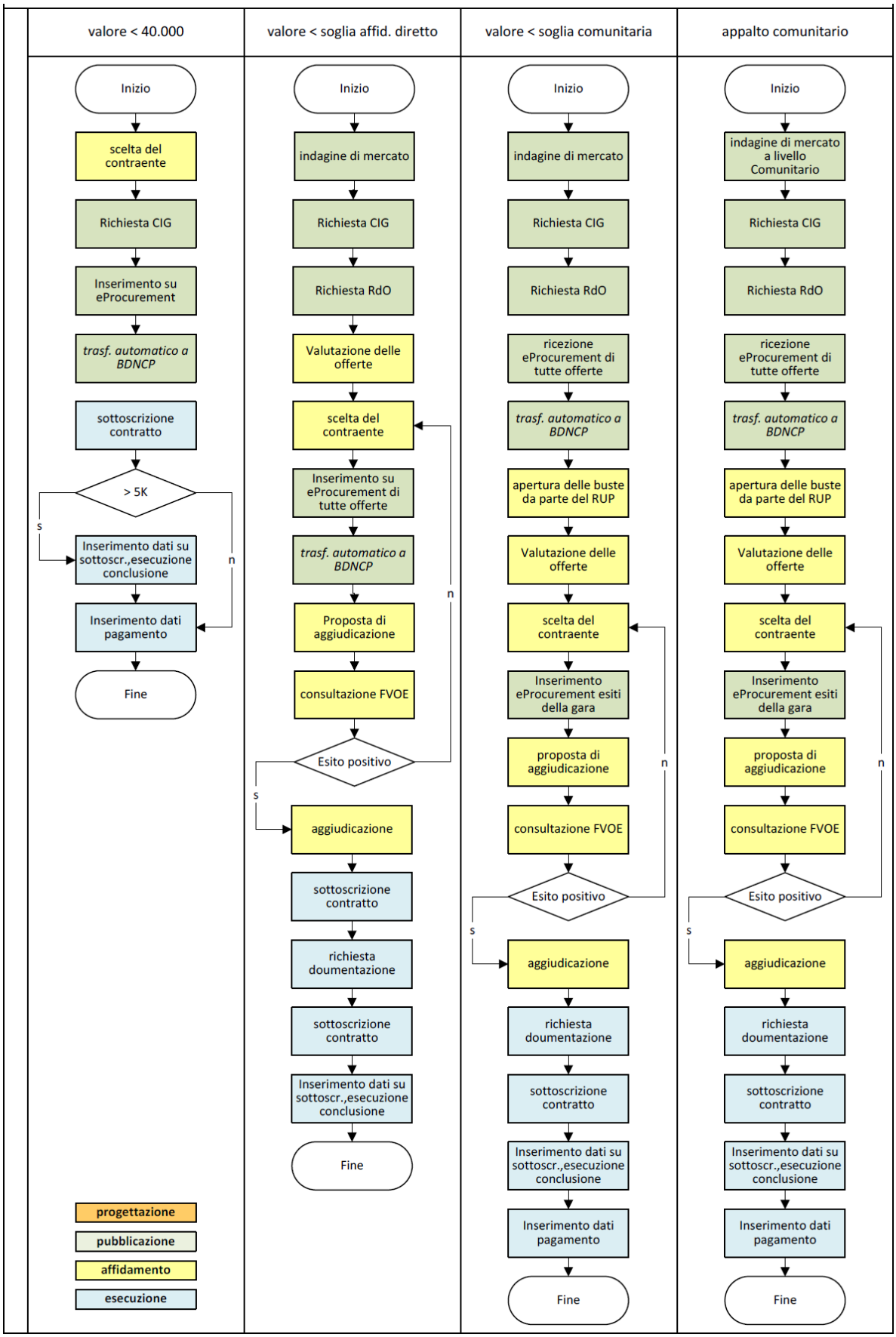

Figura 3 – Processo di eProcurement in funzione degli importi

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 varie 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 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: (i) all'offerta di beni o la prestazione di servizi ai soggetti interessati; (ii) 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*" e al "*Responsabile*" – figure già individuate nel D.Lgs. n. 196/2003 - il GDPR ha affiancato il Data Protection Officer ("*DPO*"), che deve essere nominato: (i) 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); (ii) 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; (iii) 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 introduce nuovi diritti che non erano previsti espressamente da quest'ultima quali, ad esempio, il diritto all'oblio e il diritto alla portabilità dei dati.

Va ricordato che - con il D.Lgs. n. 101 del 10 agosto 2018, contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del GDPR e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati) – sono state apportate modificazioni al D.Lgs n. 196/2003: i codici di condotta (ora rinominati "*Regole deontologiche*"), contenuti nell'Allegato A al D.Lgs. n. 196/2003 sono stati riveduti e corretti alla luce delle norme europee e riproposti all'esame del Garante per la Protezione dei dati Personali (in acronimo: "GPDP"), così come le autorizzazioni generali relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del GDPR.

I servizi resi da Udine Mercati srl interessano 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.
Si precisa esplicitamente che 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.
Vanno fornite le informative a collaboratori e loro familiari, nonché a professionisti e ditte individuali.
Infine, rimane da gestire 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.

7 ATTIVITA' SENSIBILI PER LA COMMISSIONE DI UNO DEI REATI PREVISTI DALL'ART. 25-OCTIES.1 DEL D.LGS 231/01

Le attività di Udine Mercati s.r.l. che sono state ritenute potenzialmente esposte a rischio (nella commissione dei reati previsti dall'art. 25-*octies.1* del *Decreto*), ovvero "**sensibili**", sono riconducibili in particolare alle seguenti fattispecie:

1. rapporti con la Pubblica Amministrazione in genere e con i Pubblici Poteri, anche nell'ambito di attività di vigilanza e controllo cui i medesimi sono istituzionalmente preposti;
2. rapporti commerciali, di assistenza e consulenza, di prestazione d'opera con i fornitori e/o gli outsourcer di servizi informatici/telematici;
3. rapporti con clienti, fornitori di beni e di servizi, nonché partners in genere;
4. attività di commercializzazione dei servizi della società, comprese le attività pubblicitarie, di web marketing e similari;
5. gestione pagamenti fatture;
6. accesso e controllo degli accessi ai sistemi informativi interni all'azienda.

L'Organo Amministrativo di Udine Mercati s.r.l. potrà disporre, qualora se ne ravvisi la necessità, ulteriori integrazioni delle suddette "*attività sensibili*" definendo, se del caso, gli opportuni provvedimenti operativi.

I Soggetti coinvolti nelle predette attività sensibili si ritiene possano essere gli Amministratori, il Direttore, il Delegato in materia ambientale ed in materia di igiene e sicurezza sul lavoro, i Dirigenti (ove nominati), i Responsabili amministrativi e finanziari ovvero dell'ufficio/servizio, i Responsabili amministrativi e tecnici, il personale dipendente interessato e suo diretto responsabile (secondo le rispettive competenze), gli organi

di controllo (Sindaco Unico, Revisore legale, Organismo di Vigilanza, RPCT, DPO), nonchè i consulenti e collaboratori a qualsiasi titolo coinvolti nella attività sensibile.

8 ATTIVITA' SENSIBILI PER LA COMMISSIONE DI UNO DEI REATI PREVISTI DALL'ART. 25-NOVIES DEL D.LGS 231/01

Le attività di Udine Mercati s.r.l. che sono state ritenute potenzialmente esposte a rischio (nella commissione dei reati previsti dall'art. 25-*novies* del *Decreto*), ovvero "**sensibili**", sono riconducibili in particolare alle seguenti fattispecie:

1. installazione *software* non originale;
2. accesso non autorizzato a banche dati/piattaforme pubbliche;
3. utilizzo di un numero di copie di prodotti *software* maggiore rispetto al numero consentito dalla licenza (*underlicensing*) o dalle licenze disponibili;
4. Utilizzo/diffusione di contenuti audiovisivi, immagini, foto, disegni, opere musicali e/o suoni protetti dal diritto d'autore, in assenza di accordi formalizzati per iscritto con il soggetto titolare dei relativi diritti di sfruttamento e utilizzazione economica e/o in violazione di quanto previsto dai predetti accordi.

L'Organo Amministrativo di Udine Mercati s.r.l. potrà disporre, qualora se ne ravvisi la necessità, ulteriori integrazioni delle suddette "*attività sensibili*" definendo, se del caso, gli opportuni provvedimenti operativi.

I Soggetti coinvolti nelle predette attività sensibili si ritiene possano essere gli Amministratori, il Direttore, il Delegato in materia ambientale ed in materia di igiene e sicurezza sul lavoro, i Dirigenti (ove nominati), i Responsabili amministrativi e finanziari ovvero dell'ufficio/servizio, i Responsabili amministrativi e tecnici, il personale dipendente interessato e suo diretto responsabile (secondo le rispettive competenze), gli organi di controllo (Sindaco Unico, Revisore legale, Organismo di Vigilanza, RPCT, DPO), nonchè i consulenti e collaboratori a qualsiasi titolo coinvolti nella attività sensibile.

Di seguito, si riepilogano i reati che interessano questa Parte Speciale con indicazione di esempi di condotte rilevanti

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;
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	• 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
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 minorile	600 bis c.1	Rientrano in quest'ambito: • 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-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	Rientrano in quest'ambito: • falsificare o alterare carte di credito o di pagamento o comunque ogni altro strumento di pagamento diverso dai contanti; • detenere, acquistare o cedere carte di credito o di pagamento o comunque ogni altro strumento di

		pagamento diverso dai contanti che siano di provenienza illecita o comunque falsificati o alterati.
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 contanti, se la pena della reclusione 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-quater	Rientrano in quest'ambito: • produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, siano costruiti principalmente per commettere reati attraverso mezzi di pagamento diversi dai contanti o siano specificamente adattati al medesimo scopo
Frode informatica (nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale)	640 ter	Rientrano in quest'ambito: • alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti
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 contanti, se la pena della reclusione è inferiore a 10 anni.		
25-octies. 1 c. 2 bis (da 250 a 600 quote)	**Art. C.P.**	
Trasferimento fraudolento di valori	512 bis	Rientrano in quest'ambito: • nominare fittiziamente un prestanome come amministratore di una società, al quale sia attribuita la titolarità del conto corrente bancario della società, con potere di disporre delle risorse della medesima
25-novies (fino a 500 quote)		
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 l'elusione	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 accordi di licenza

funzionale di dispositivi applicati a protezione di Software. Violazione diritto d'autore in relazione a banche dati.		(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

9 IL SISTEMA DEI CONTROLLI

La Società, nell'adeguare la presente Parte Speciale ai reati previsti dagli artt. 24-*bis*, 25-*quinquies*, 25-*octies.1* e 25-*novies* del D.Lgs n. 231/2001, ha 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 al D. Lgs. 196/2003, come modificato dal D.Lgs. 51/2018;
- 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.

Si evidenzia che costituiscono parte integrante dei sistemi di controllo di Udine Mercati s.r.l. rispetto alle attività a rischio i seguenti elementi:

- Parte Generale del Modello Organizzativo;

- Codice Etico e Valori Condivisi;
- Sistema anticorruzione adottato;
- Sistema di Deleghe, Procure e Poteri;
- Struttura Organizzativa (Organigramma e mansionario);
- Principi e Regole generali di comportamento di cui alla presente Parte Speciale;
- Procedure ed istruzioni operative collegate ai reati presupposto di cui alla presente Parte Speciale.
- Regolamenti e moduli interni;
- Sistema Disciplinare;
- Policy Whistleblowing;
- Regolamento Aziendale – "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei*";
- Regolamento Aziendale – "*Manuale Organizzativo privacy*".

9.1 Il Codice Etico ed i valori condivisi

Udine Mercati s.r.l. si è dotata inoltre 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)[36] di applicazione generale a tutte le pubbliche amministrazioni, cui Udine Mercati S.r.l. 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[37].

Il Codice Etico di Udine Mercati s.r.l. 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 Udine Mercati s.r.l..

La piena effettività del Codice Etico è garantita anche dal fatto che ogni scostamento dai valori e dai principi in esso contenuti, potrebbe originare una responsabilità a livello disciplinare.

In generale, al fine di prevenire ed impedire il verificarsi dei reati presupposto trattati nella presente Parte Speciale, tutti i *Destinatari* del Modello **devono**:

- rispettare le Leggi e Regolamenti a livello Europeo, Statale, Regionale e Locale;
- rispettare i principi di:

[36] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:2013-04-16;62

[37] 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

- Legalità ed Integrità: rispetto di leggi, regolamenti ma anche integrità morale, che si traduce nell'agire in modo corretto e trasparente, evitando informazioni ingannevoli e comportamenti tali da trarre indebito vantaggio da posizioni di debolezza o di non conoscenza altrui;
- Correttezza, lealtà ed onestà: rapporti corretti con tutti gli interlocutori, cui fornire tutti gli elementi per scegliere ed agire liberamente ed in maniera informata;
- Fedeltà e Prevenzione del conflitto di interessi: l'interesse primario e superiore del bene aziendale non deve essere messo a rischio da fenomeni opportunistici;
- Antiriciclaggio e Anticorruzione: la Società rispetta e si pone a baluardo delle strutture pubbliche e del loro operato, anche in termini di controllo, perseguendo obiettivi di contrasto ad ogni forma di influenza nell'azione legittima dei pubblici funzionari e di privati, nonché adottando pedissequamente e proattivamente ogni comportamento che contrasti il riciclaggio e l'autoriciclaggio;
- 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;
- Trasparenza, completezza dell'Informazione e tracciabilità: ogni azione deve essere svolta, garantendo correttezza, completezza, uniformità, trasparenza e tempestività d'informazione e ogni scelta deve essere adeguatamente documentata;
- Tutela del patrimonio e delle risorse dell'Ente: la Società non può svilire il proprio patrimonio e deve preservarlo con idonei interventi.

Tutti i soggetti appartenenti - direttamente o indirettamente - all'organizzazione aziendale della Società (amministratori, apicali, subordinati, collaboratori, consulenti, partners, ecc.) **sono tenuti**:

- a prestare il necessario impegno al fine di prevenire la possibile commissione dei reati trattati nella presente Parte Speciale, riferendo con tempestività e riservatezza al Direttore, ovvero all'Organo Amministrativo – e, in caso di conflitto di interessi, al Sindaco Unico - nonché all'Organismo di Vigilanza e (ove necessario) al RPCT, di ogni notizia di cui siano venuti a conoscenza

nell'espletamento delle proprie attività, circa violazioni di norme giuridiche, del Codice Etico e del presente Modello, nonché di altre disposizioni aziendali che possano, a qualunque titolo, coinvolgere la Società;

- 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;
- al rispetto delle procedure legate ad un utilizzo corretto dei dati, nel pieno rispetto delle norme a Protezione dei Dati Personali e della normativa vigente che va oltre ai Dati Personali ove applicabile (Regolamento (EU) 2016/679 – c.d. "*GDPR*", del D.Lgs. n. 196/03 c.d. "*Codice Privacy*" e dei Pronunciamenti dell'Autorità Garante per la Protezione dei Dati Personali; Regolamento (EU) – "*Data Governance Act*"; Regolamento (EU) 2023/2854 c.d. "*Data Act*"; Regolamento (EU) 2024/1689 c.d. "*Artificial Intelligence Act"*).

10 DELEGHE, PROCURE E POTERI DI FIRMA

È stato nominato il Direttore di Mercato ai sensi del vigente *"Regolamento del Mercato Agroalimentare all'Ingrosso di Udine"* approvato dal Comune di Udine, i cui titoli, competenze ed esperienze garantiscono la sua capacità tecnica ed organizzativa, per la gestione e le attività ivi previste.

Per le aree di attività potenzialmente interessate da condotte suscettibili di integrare i reati presupposto di cui alla presente Parte Speciale, in particolare l'Organo Amministrativo ed il Direttore potrebbero essere chiamati a rispondere a titolo personale e/o in concorso di eventuali reati.

Qualora sia necessaria l'attribuzione di procure, l'Organo Amministrativo delibererà il rilascio ai soggetti di specifica procura scritta che rispetti i seguenti criteri:

- ciascuna procura deve definire in modo specifico e inequivocabile i poteri del procuratore e il soggetto cui il procuratore riporta gerarchicamente;
- i poteri gestionali assegnati con le procure e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il procuratore deve disporre di poteri di spesa adeguati alle funzioni conferitegli;
- le procure devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi.

Nel caso di incarico assegnato a collaboratori, consulenti o altri ad operare in rappresentanza o nell'interesse della Società, deve essere prevista la forma scritta e deve essere inserita una specifica clausola contrattuale che vincoli all'osservanza del presente Modello.

11 STRUTTURA ORGANIZZATIVA

Gli Organi Sociali previsti dallo Statuto di Udine Mercati s.r.l. sono i seguenti:

- Assemblea degli azionisti;
- Amministratore unico / Consiglio di Amministrazione;
- Amministratore delegato;
- Organo di Controllo (Sindaco Unico);
- Comitato Tecnico Consultivo.

Attualmente la Società è amministrata da un Consiglio di Amministrazione. L'atto di nomina è costituito da una delibera dell'Assemblea che è coerentemente riportata in Camera di Commercio e desumibile dalla Visura Camerale. Secondo lo Statuto, il Consiglio di Amministrazione/Amministratore unico dura in carica da uno (1) a tre (3) esercizi sociali ed è rieleggibile.

E' presente il Sindaco unico, con funzione anche di revisore legale dei conti.

L'Assemblea degli Azionisti, attualmente costituita da rappresentanti di Enti Pubblici e privati, oltre a decidere su operazioni particolari quali la cessione e la dismissione di rami d'azienda per l'esercizio dei servizi pubblici affidati, la cessione o dismissione di partecipazioni in società controllate o collegate, l'acquisto di partecipazioni societarie, procede alla nomina dell'Amministratore unico ovvero dei componenti del Consiglio di Amministrazione e del suo Presidente, nonché sulla determinazione del loro compenso.

12 PRINCIPI GENERALI

Al fine di costruire idoneo a prevenire la commissione di reati, la Società ha ritenuto ineludibile adottare alcuni presidi generali che si traducono nella promulgazione diffusione di un se di valori sui quali fonda la propria azione (Codice Etico,) ma anche nella predisposizione di vincoli all'azione stessa, per ovviare o comportamenti suscettibili di integrare le fattispecie di reato trattate nella presente Parte Speciale e nella chiara indicazione delle dipendenze gerarchiche delle diverse posizioni organizzative. Rimangono da definire alcuni comportamenti che trasformano la posizione organizzativa in un ruolo: alcuni di essi sono di carattere generale, mentre altri sono più specifici per situazioni codificabili.

Nell'ambito comportamenti più generali, va ricordato che il *Personale* ed il *Personale Apicale*, nonché i componenti degli *Organi di Controllo* (nelle accezioni di cui alle definizioni del superiore paragrafo 1.1) **sono tenuti:**

- a conoscere e rispettare la normativa italiana e straniera applicabile;
- a conoscere la struttura organizzativa aziendale;
  a conoscere le norme inerenti il sistema amministrativo, contabile, finanziario e di reporting della Società;
- a conoscere il Codice Etico;

- a conoscere le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti;
- a conoscere i regolamenti e i provvedimenti delle Autorità di controllo;
- a prestare il necessario impegno al fine di prevenire la possibile commissione di reati, riferendo con tempestività e riservatezza al Direttore, ovvero all'Organo Amministrativo (ovvero al Presidente del CdA) e all'Organismo di Vigilanza - nonché, ove di interesse, anche al Responsabile per la Prevenzione della Corruzione e per la Trasparenza - ogni notizia di cui siano venuti 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 ai sensi del D.Lgs n. 231/2001;
- 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;
- al rispetto delle procedure legate alla tutela dell'ambiente di lavoro e della Sicurezza, in conformità alle norme vigenti;
- a verificare e garantire la tempestività e adeguatezza dei flussi informativi verso l'Organismo di Vigilanza.

13 REGOLE GENERALI DI COMPORTAMENTO

Richiamato il contenuto dell'analisi del rischio di cui all'allegato "*Risk assessment*" della Parte Generale, si illustra di seguito – in via meramente esemplificativa – quali sono le regole generali di comportamento previste ed ineludibili da seguire quando non sono previste diverse specifiche procedure e ferme le previsioni del Codice Etico, del "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei"*, del "*Manuale Organizzativo privacy"* e della presente Parte Speciale.

I seguenti **divieti** ed **obblighi** di carattere generale si applicano agli Amministratori, al Direttore, ai Dirigenti e Dipendenti e – in generale – al *Personale* di Società, in via diretta, nonché ai Collaboratori, Consulenti e *Business Partners* a qualsiasi titolo della Società.

È fatto espresso **divieto** di:

- porre in essere, dare collaborazione o dare causa alla realizzazione di atti o comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle trattate nella presente Parte Speciale;
- porre in essere atti o comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di resto rientranti tra quelle precedentemente elencate, possano potenzialmente diventarlo;
- tenere un comportamento non corretto né trasparente, che ostacoli il pieno rispetto di norme di Legge e regolamenti nonché delle procedure interne aziendali;

- adottare atti o comportamenti contrari alla normativa vigente, anche mediante l'affidamento di incarichi a professionisti esterni e soggetti terzi, per favorire indebitamente la Società;
- falsificare, contraffare o modificare in qualsiasi modo le registrazioni e la documentazione al fine di mostrare un artificioso rispetto delle norme;
- ricorrere ad appaltatori/outsourcer che non diano idonea garanzia del rispetto della normativa;

È fatto espresso **obbligo** di:

- improntare la propria condotta ai principi generali del Codice Etico, con particolare riferimento ai principi di legalità, correttezza, tracciabilità e trasparenza;
- svolgere le attività sensibili conformemente alle leggi vigenti, alle norme generali del Codice Etico, nonché alle disposizioni aziendali, alle specifiche procedure previste dalla Società a presidio dei rischi di commissione dei reati di cui alla presente Parte Speciale;
- mantenere la 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 o di collaborazione o contrattuale in genere;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti (cartacei od informatici) o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Sindaco Unico e/o del revisore legale e/o di altri soggetti comunque incaricati del controllo (fra cui Organismo di Vigilanza e Responsabile per la Prevenzione della Corruzione e per la Trasparenza);
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza, nonché omettere la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;
- effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari;
- porre in essere qualsiasi comportamento di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione da parte di Autorità pubbliche.

In particolare gli esponenti della Società che hanno fra le loro mansioni il controllo in relazione ai reati trattati nella presente Parte Speciale (compreso il Direttore) – di fatto od anche sulla base di specifica procura conferita dall'Organo Amministrativo - devono sempre comportarsi in maniera conforme ai principi sanciti nel Codice Etico e alle previsioni del presente Modello.

Essi, in particolare, **dovranno:**

1. avere una conoscenza adeguata della normativa di cui ai D.Lgs. n. 231/2001 e D.Lgs. n. 24/2023 e s.m.i., nonché di quanto riportato nel Modello e nel Codice Etico adottati dalla Società;

2. avere una conoscenza adeguata del "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei"* e del "*Manuale Organizzativo privacy"* adottati dalla Società;
3. avere una conoscenza adeguata della normativa di cui al Regolamento (EU) 2016/679 – c.d. "*GDPR*", e al D.Lgs. n. 196/2003 c.d. "*Codice Privacy*", ss.mm.ii., nonchè dei Pronunciamenti dell'Autorità Garante per la Protezione dei Dati Personali (ed altresì, ove e quando applicabili alla Società, anche al Regolamento (EU) – "*Data Governance Act*", al Regolamento (EU) 2023/2854 c.d. "*Data Act*" ed al Regolamento (EU) 2024/1689 c.d. "*Artificial Intelligence Act"*)
4. fornire, ai propri collaboratori e subordinati, direttive sulle modalità di condotta operativa da adottare nello svolgimento delle rispettive mansioni, nel loro ambito di attività, trasferendo loro la conoscenza dei principi ed aspetti del D.Lgs. n. 231/2001, di quanto riportato nel Modello, nel Codice Etico, delle previsioni di cui ai superiori punti 1. - 2. - 3. e presentando le principali aree di rischio;
5. verificare la conformità della propria azione alle regole di comportamento di cui alla presente Parte Speciale e relative procedure/regolamenti (in particolare al "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei"* ed al "*Manuale Organizzativo privacy"*;
6. verificare e garantire la segregazione delle funzioni: ovvero la separazione tra soggetto che decide, quello che autorizza, quello che esegue e quello che controlla;
7. verificare e garantire che l'assegnazione dei poteri, nell'ambito del processo decisionale, sia coerente con le posizioni gerarchiche, l'autonomia e la responsabilità;
8. verificare e garantire l'adeguatezza dei controlli in tutte le fasi dei processi;
9. verificare e garantire completezza, tempestività ed adeguatezza dei flussi informativi verso l'Organo di Vigilanza.

14 REGOLE DI COMPORTAMENTO PER LA PREVENZIONE DEI REATI PREVISTI DALL'ART. 24-bis DEL D.LGS. 231/01

Le presenti regole sono state predisposte con l'intento di prevenire il coinvolgimento di Udine Mercati s.r.l. nei reati di cui all'art. 24-*bis* del D.Lgs. n. 231/2001[38], ovvero il compimento di alcune delle predette condotte criminose nell'interesse o a vantaggio della Società stessa.

14.1 Protezione Hardware e Software

Per rispondere ai dettami normativi in materia di trattamento, la struttura ha adottato opportune misure di sicurezza organizzative, procedurali e tecniche.

[38] Vedasi nota 3.

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 Sistema Informativo della Società.

14.2 La policy sul trattamento dati e sull'utilizzo degli strumenti

Udine Mercati s.r.l. si è dotata di regolamenti denominati " *Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei"* e "*Manuale Organizzativo privacy"* approvati dall'Organo Amministrativo e che costituiscono parte integrante della presente Parte Speciale.
Tali regolamenti sono stati sviluppati 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. 196/2003, e s.m.i.).
Le indicazioni contenute nei citati documenti sono valide anche per ciò che attiene la prevenzione dei reati di cui al D.Lgs. n. 231/2001.
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 Udine Mercati s.r.l. 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.

I citati regolamenti contengono, 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 Udine Mercati s.r.l. su computer diversi da quello in uso;
- non consentire a chiunque esterno all'azienda di collegare il proprio computer alla rete aziendale senza previa autorizzazione del Direttore e/o dell'Organo Amministrativo.
- 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 Udine Mercati s.r.l. ;
- evitare di condividere documenti e file in genere con il computer personale o di altri;
- avvisare immediatamente il Direttore e/o l'Organo Amministrativo 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 il Direttore e/o l'Organo Amministrativo qualora venga indebitamente sottratto il proprio computer o qualsiasi altro dispositivo utilizzato per connettersi alla rete di Udine Mercati s.r.l..

14.2 Persone

Nell'attuale contesto in cui le aziende si trovano ad operare, i confini aziendali si mostrano sfumati e l'azienda ricorre frequentemente ad outsourcer e partner, costituendo con essi rapporti che vanno oltre la mera fornitura. Si tratta, quindi, di definire regole e principi che stabiliscono anche un riferimento per chi opera esternamente all'azienda ma, in qualche modo, ne costituisce una propaggine organizzativa.

Nei prossimi paragrafi troveranno spazio le modalità operative che Udine Mercati s.r.l. ritiene di adottare per definire come le risorse interne e le organizzazioni o le risorse esterne devono operare perché sia gestito il rischio di commissione di reati presupposto.

14.3 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 allegata alla presente Parte Speciale.

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 provvede a formalizzare una delega al Direttore 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 dell'Ente 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 Udine Mercati s.r.l. 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. Esistono contratti per la fornitura di servizi Cloud, stipulati con primari interlocutori.

All'interno dell'azienda i soggetti autorizzati alla firma custodiscono personalmente il proprio dispositivo di firma.

14.4 Hardware, Software e Servizi a Valore Aggiunto

L'istallazione di nuove apparecchiature IT o la creazione/modifica di procedure deve essere formalmente approvata dal Direttore e/o dall'Organo Amministrativo. L'approvazione include il parere favorevole del 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, deve essere sempre formalizzato, a vale di 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 Direttore e il Delegato devono essere informati di problemi ai sistemi di elaborazione, per verificare che la sicurezza del patrimonio informativo non sia stata pregiudicata e ogni evento rilevante deve essere 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 previsto 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, in ciascun contratto di outsourcing, deve essere previsto l'inserimento di clausole formalizzate che consentano alla Società di svolgere audit in materia di sicurezza informatica presso l'outsourcer stesso.

15 REGOLE DI COMPORTAMENTO PER LA PREVENZIONE DEI REATI PREVISTI DALL'ART. 25-octies.1 DEL D.LGS. 231/01

Le presenti regole sono state predisposte con l'intento di prevenire il coinvolgimento di Udine Mercati s.r.l. nei reati di cui all'art. 25-*octies.1* del D.Lgs. n. 231/2001, ovvero il compimento di alcune delle predette condotte criminose nell'interesse o a vantaggio della Società stessa.

<u>Con riferimento alle attività di gestione dei pagamenti</u>:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori,

anche stranieri (attraverso l'amministrazione, l'aggiornamento e il monitoraggio del relativo elenco storico);

- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;
- assicurare, in caso di pagamenti a favore di soggetti terzi tramite bonifico bancario, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta;
- operare nel rispetto delle rispettive procedure per quanto concerne i pagamenti con Carta di Credito, oltre che nel rispetto dei limiti delle deleghe e delle procure conferite in tale ambito;
- in caso di pagamento a carico della Società a mezzo di carta di credito, impiegare esclusivamente la carta di credito aziendale o altro strumento comunque intestato alla Società o a persona fisica in sua rappresentanza;
- assicurare un adeguato sistema di segregazione dei poteri autorizzativi, di controllo ed esecutivi in relazione alla gestione dei pagamenti delle fatture e alle modalità di predisposizione ed approvazione delle relative distinte di pagamento;
- operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;
- segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità (i.e. a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura).

Con riguardo all'utilizzo delle apparecchiature informatiche/software:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;
- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società, informare tempestivamente il responsabile della funzione competente alla gestione dei relativi

sistemi/dispositivi informatici e attenersi alla specifica procedura contenuta nel "*Manuale Organizzativo privacy"* per la gestione delle violazioni dei dati personali (*data breach notification*);

- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- impiegare sulle apparecchiature della Società soltanto prodotti ufficialmente acquisiti dalla Società;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di Udine Mercati S.r.l.;
- in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

16 REGOLE DI COMPORTAMENTO PER LA PREVENZIONE DEI REATI PREVISTI DALL'ART. 25-novies DEL D.LGS. 231/01

Le presenti regole sono state predisposte con l'intento di prevenire il coinvolgimento di Udine Mercati s.r.l. nei reati di cui all'art. 25-*novies* del D.Lgs. n. 231/01, ovvero il compimento di alcune delle predette condotte criminose nell'interesse o a vantaggio della Società stessa.

In relazione al reato di cui sopra, vi è l'espresso **obbligo** a carico dei destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività inerenti l'utilizzo dei sistemi informatici aziendali;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste ai sensi delle procedure aziendali nei confronti delle funzioni preposte alla gestione dei sistemi informatici e dell'OdV, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste eventualmente esercitate.

È fatto **divieto**, in particolare, di:

a) installare programmi software diversi da quelli messi a disposizione e autorizzati dalla Società;

b) scaricare da Internet programmi senza la preventiva autorizzazione della Società, nella persona dell'amministratore di sistema;

c) caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;

d) d) acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;

e) e) detenere supporti di memorizzazione non originali (DVD\CD\floppy);

f) installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;

g) utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

h) utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;

i) distribuire il software aziendale a soggetti terzi;

j) accedere illegalmente e duplicare banche dati.

17 SISTEMA DISCIPLINARE

La Società ha adottato un *Sistema Disciplinare* che è stato diffuso a tutti i Destinatari e che viene applicato al fine di sanzionare il mancato rispetto delle misure indicate nel Modello, nel Codice Etico e nella *Policy Whistleblowing* ex D.Lgs 24/2023 adottati. Tale sistema sanzionatorio è parte integrante del presente Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001 e s.m.i. della Società e quest'ultima intende applicare con costanza le sanzioni ivi previste in caso di mancato rispetto delle misure indicate nel Modello e dissuadere ogni comportamento che violi il rispetto delle misure preventive e protettive adottate per la prevenzione dei reati di cui alla presente Parte Speciale.

18 POLICY WHISTLEBLOWING

Rientra tra i meccanismi di controllo interni anche il sistema di *Whistleblowing*, come attuato in Udine Mercati s.r.l.. Esso – anche in ragione dell'estensione dell'onere di segnalazione delle condotte rilevanti ai sensi del D.Lgs. n. 231/2001, ovvero di violazioni del Modello di Organizzazione, Gestione e Controllo della Società di cui si sia venuti a conoscenza nell'esercizio delle proprie funzioni, compresi i fondati sospetti, riguardanti le violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse in Società, nonché degli elementi riguardanti condotte volte ad occultare tali violazioni (art. 2 del D.Lgs n. 24/2023) realizzato attraverso le previsioni del Codice Etico – costituisce un presidio fondamentale di legalità dell'azione sociale. L'effettività e il corretto funzionamento dell'istituto sono affidati alle disposizioni della *Whistleblowing Policy* adottata dalla Società – e cui si rimanda integralmente - mentre le previsioni del Sistema Disciplinare assicurano ad un tempo sia la tutela di coloro che segnalano l'esistenza di comportamenti contrari alla legge e/o al pieno funzionamento del Modello di Organizzazione, Gestione e Controllo ex D.Lgs n. 231/2001, sia il corretto utilizzo dell'istituto (sanzionandone un impiego "deviato" o comunque animato da finalità incompatibili con la logica del *Whistleblowing*).

19 SISTEMA DI CONTROLLO SULL'ATTUAZIONE DEL MODELLO E SUL MANTENIMENTO NEL TEMPO DELLE CONDIZIONI DI IDONEITÀ DELLE MISURE ADOTTATE

Al fine di prevenire la commissione dei reati indicati nei precedenti paragrafi, la Società ha predisposto e implementato appositi presidi organizzativi e di controllo al fine di prevenire e controllare il rischio di commissione dei reati nello svolgimento delle attività a rischio individuate.

Tutte le funzioni coinvolte in tali attività sono tenute ad osservare le disposizioni di legge esistenti in materia, le prescrizioni previste dal D.Lgs. n. 231/2001, nonché quanto previsto dal Modello di Organizzazione, Gestione e Controllo e dal Codice Etico adottati dalla Società.

19.1 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 la sede sociale 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 l'osservanza, l'attuazione e l'adeguatezza del Modello (Parte Generale e Parti Speciali) in ottica di prevenzione della commissione dei reati individuati nella presente Parte Speciale;
- vigilare sull'effettiva applicazione della Parte Generale e delle Parti Speciali del Modello, nonchè rilevare deviazioni comportamentali dei soggetti destinatari qualora riscontrati dall'analisi dei flussi informativi e dalle segnalazioni ricevute;

- proporre che vengano emanate ed aggiornate istruzioni standardizzate, relative ai comportamenti da seguire nell'ambito delle aree/attività a rischio, come individuate anche nella presente Parte Speciale;
- svolgere ogni accertamento ritenuto opportuno su singole operazioni esposte a rischio o in relazione al flusso informativo;
- svolgere verifiche periodiche sul rispetto delle procedure interne e del "sistema" di controllo in relazione ai reati, comportamenti ed alle regole trattati nella presente Parte Speciale;
- indicare al management ogni opportuna modifica e innovazione nelle procedure aziendali, volte a una migliore prevenzione del rischio di commissione di reati;
- esaminare eventuali segnalazioni specifiche 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:
    a) all'osservanza da parte dei Destinatari dei contenuti del Modello e del Codice Etico;
    b) alla possibilità per la Società di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
    c) all'attuazione di meccanismi sanzionatori (quali la risoluzione del contratto nei riguardi di Fornitori, Appaltatori, Consulenti e Outsourcer) qualora si accertino violazioni delle prescrizioni;
- accertare ogni eventuale violazione della presente Parte Speciale e proporre eventuali sanzioni disciplinari.

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

- svolgere verifiche periodiche sul rispetto delle procedure interne e del "sistema" di controllo in ambito informatico e di trattamento dei dati, sul diritto d'autore e sulla prevenzione dei reati a sfondo pornografico e pedopornografico;
- 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.

I risultati dell'attività di vigilanza e controllo sono comunicati dall'OdV all'Organo Amministrativo nella propria Relazione annuale, ovvero tempestivamente allorquando ricorrano particolari esigenze o a discrezione dell'OdV stesso.

I Destinatari della presente Parte Speciale dovranno collaborare con l'Organismo di Vigilanza (oltre che con il Responsabile per la Prevenzione della Corruzione e per la Trasparenza) rispondendo prontamente a tutte

le richieste degli stessi, fornendo loro la documentazione e le informazioni di cui sono a conoscenza, contribuendo, secondo le proprie competenze, a predisporre ed applicare puntualmente le procedure che descrivono i comportamenti da adottare nell'ambito delle attività sensibili e dei processi strumentali.

20 FLUSSI INFORMATIVI DALL'ODV

Fermo quanto previsto dallo Statuto dell'Organismo di Vigilanza, quest'ultimo riferisce - in particolare - in merito ad ispezioni, controlli, segnalazioni e provvedimenti al Direttore, nonché – in ipotesi di conflitto di interessi, inerzia o concorso nella violazione – all'Organo Amministrativo e/o all'Assemblea dei Soci ed al Sindaco Unico.

In caso di violazione delle norme di legge e/o della presente Parte Speciale e/o di procedure e protocolli 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 Direttore e l'Organo Amministrativo, nonché - in ipotesi di conflitto di interessi, inerzia o concorso nella violazione - l'Assemblea dei Soci e/o il Sindaco Unico, al fine di permettere agli stessi di agire assumendo i provvedimenti ritenuti opportuni.

La programmazione delle attività di controllo è svolta dall'OdV secondo quanto prescritto dallo Statuto dell'Organismo di Vigilanza.

21 FLUSSI INFORMATIVI VERSO L'ODV

L'Organo Amministrativo, il Direttore, il Delegato in materia ambientale, il Datore di Lavoro ed il delegato dal datore di lavoro ai sensi dell'art. 16 del D.Lgs n. 81/2008, gli eventuali Responsabili delle Aree aziendali interessate, il Delegato in materia di Sistemi Informatici, il Sindaco Unico, nonché il RSPP, il RPCT ed il DPO — nell'ambito delle proprie competenze e funzioni — devono inviare all'OdV, con tempestività ove ricorra un fatto di rilievo, ogni dato, informazione, documentazione aggiornamento, avente rilevanza fattuale o di natura giuridica, attinente, strumentale od oggetto dell'azione prevenzionistica della commissione dei reati di cui alla presente Parte Speciale.

Chiunque può rivolgersi all'OdV in qualsiasi momento, nei modi previsti dallo Statuto dell'Organismo di Vigilanza, sia per segnalare fatti e/o notizie rilevanti ai fini della prevenzione dei reati previsti del *Decreto* sia per suggerire proposte ed interventi.

Come previsto dalla Parte Generale del Modello Organizzativo della 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 dedicato 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, con le rispettive periodicità, alcuni aspetti da comunicare all'OdV.

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 nell'anno in corso, entro il 31 dicembre di ogni anno, il soggetto incaricato dovrà inviare una comunicazione all'OdV evidenziando l'assenza di eventi alla voce specifica per l'anno di riferimento (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/DIRETTORE/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/DIRETTORE/DELEGATO	AD EVENTO
4	Evento, situazione, condizione che compromette la capacità di elaborazione	DIRETTORE/DELEGATO	AD EVENTO
5	Mappatura del Sistema Informativo	DELEGATO	AD EVENTO
6	Sistema di Autorizzazione al trattamento	DELEGATO	AD EVENTO
7	Modifiche nei software gestionali	DELEGATO	ANNUALE

21.1 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); • *Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei*; • *Manuale Organizzativo privacy*; • 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/Sindaco Unico e del RPCT; • Giustificabilità degli algoritmi; • Accountability.

22 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.

22.1 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.

22.2 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.

22.3 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.

22.4 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.

22.5 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.

22.6 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.

22.7 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.

23 DOCUMENTAZIONE AZIENDALE DI RIFERIMENTO

- Regolamento approvato dal Comune di Udine;
- Parte Generale;
- Codice Etico e Valori Condivisi;
- Sistema anticorruzione adottato;
- Sistema di Deleghe, Procure e Poteri;
- Atto di nomina del Data Protection Officer;
- Struttura Organizzativa (Organigramma e mansionario in materia di sistemi informatici e trattamento dati);
- Principi e Regole generali di comportamento di cui alla presente Parte Speciale;
- Procedure ed istruzioni operative collegate ai reati presupposto di cui alla presente Parte Speciale.
- Regolamenti e moduli interni;
- Sistema Disciplinare;
- Policy Whistleblowing;
- Regolamento Aziendale – "*Regolamento interno per l'utilizzo consapevole della strumentazione informatica e della rete internet e per la gestione degli archivi cartacei"*;
- Regolamento Aziendale – "*Manuale Organizzativo privacy"*.

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 Udine.