PARTE SPECIALE "G":
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

relativo al

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

adottato da

DANIELE AMBIENTE S.R.L
Versione Giugno 2025 (Rev.1/25)

Premessa e introduzione

La presente Parte Speciale è dedicata ai reati informatici previsti dall'art. 24-bis del Decreto, introdotto dall'art. 7 della legge 18 marzo 2008, n. 48. Si tratta di reati commessi mediante l'impiego di tecnologie informatiche o telematiche e caratterizzati da diverse tipologie di condotta.

Alcuni di questi reati sono connotati dall'uso illegittimo degli strumenti informatici e finalizzati all'accesso abusivo in un sistema informatico, alla modifica o al danneggiamento dei dati ivi contenuti, ovvero al danneggiamento del medesimo. Altri riguardano condotte di intercettazione illegittima di comunicazioni informatiche o telematiche. Infine, è prevista la fattispecie di frode informatica del soggetto certificatore della firma elettronica.

Reati informatici e D.Lgs. 231/2001: uno sguardo normativo

L'art 6 comma 2 lett. b) del D.Lgs. 231/2001, individua la definizione di MOG dell'Ente, e stabilisce che questi debbano "prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire".

È una normativa sostanzialmente sanzionatoria, poiché le regolamentazioni specifiche sono previste in altre normative di riferimento.

Il D.Lgs. 231/2001 ha il compito di guidare le società che sono dotate di un Modello di organizzazione, gestione e controllo nell'applicazione di protocolli per il pieno rispetto delle normative cogenti e per l'implementazione di standard sempre più elevati, in particolare nel delicato ambito della sicurezza sul lavoro.

L'art. 24 bis del D.Lgs. 231/2001, rubricato "Delitti informatici e trattamento illecito di dati" pone in evidenza che i reati informatici commessi nell'interesse o vantaggio dell'Ente da parte di soggetti apicali o preposti ne determinano la responsabilità amministrativa dell'ente stesso.

In questa prospettiva, colpisce che il legislatore nazionale non abbia inteso inserire nell'elenco dei c.d. reati-presupposto i delitti previsti dal "Codice della privacy", ossia dal D.Lgs. 196/2003, anche inseguito alla rivisitazione delle fattispecie effettuata nel 2018, con l'adozione del D.Lgs. 101/2018.

Va rilevato, peraltro, che i reati previsti dall'art. 24 bis D.lgs. 231/2001 sono, sostanzialmente, tutte ipotesi di data breach dolosi o di violazioni informatiche con implicazioni anche in tema di trattamento dei dati.

L'attuazione di una *privacy compliance* deve certamente valutare i rischi di violazioni dolose rientranti nelle fattispecie di cui all'art. 24 bis D.Lgs. 231/2001, ma anche di quelle previste dal D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018. L' altro elemento rilevante è la previsione della procedura di whistelblowing, prevista dalla L. 179/2017.

La procedura di whistleblowing, infatti, volta alla minimizzazione e bilanciamento tra diritto del whistelblower a non subire ritorsioni e del soggetto chiamato in causa a conoscere anche la fonte degli addebiti mossigli.

Secondo il testo della Legge 48/2008 si possono identificare tre gruppi distinti di reati, per ognuno dei quali si specificano le sanzioni irrogabili, sia pecuniarie che interdittive:
a) il primo gruppo comprende gli articoli 615 ter, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater e 635 quinquies c.p.

La caratteristica comune ai reati previsti dagli articoli citati, consiste nel punire il danneggiamento di hardware, di software e di dati: viene punito l'accesso abusivo ad un sistema e l'intercettazione o l'interruzione di dati compiute attraverso l'installazione di appositi software o hardware e viene punita come aggravante la commissione degli stessi reati in sistemi informatici di pubblica utilità;
b) il secondo gruppo di reati è costituito dagli artt. 615 quater e 615 quinquies c.p.: tali articoli puniscono la detenzione e la diffusione di software e/o di attrezzature informatiche atte a consentire la commissione dei reati di cui alla precedente lett. a);
c) il terzo gruppo di reati comprende i reati di cui agli artt. 491 bis e 640 quinquies c.p.: viene punita la violazione dell'integrità dei documenti informatici e della loro gestione attraverso la falsificazione di firma digitale (elettronica).

Non tutti i reati informatici sono stati presi in considerazione dalla Legge 48/2008 e, pertanto, non figurano fra i reati presupposti ex d.lgs. 231/01: si tratta di condotte direttamente collegate a quelle invece prese in considerazione, come ad esempio la violenza esercitata su programmi

informatici attraverso l'introduzione di un virus o la loro alterazione (art. 392 c.p.).Ciò può avvenire per diretta conseguenza di un accesso abusivo o della illegittima detenzione di software o di codici d'accesso, reati già puniti dagli articoli indicati alla precedente lett. a). Esiste poi una serie di reati che vengono compiuti per commettere un altro reato informatico: ad esempio, la sostituzione di persona (art. 494 c.p.); infatti è assolutamente normale nella commissione di un reato informatico che chi lo commette utilizzi abusivamente l'identità informatica di chi ha diritto all'accesso ad un sistema per poter realizzare un accesso abusivo. A questi reati se ne possono aggiungere degli altri: ad esempio, qualora il danneggiamento riguardi come si è detto, un server di posta elettronica, si incorre anche nella violazione degli artt. 616 e 617 c.p.; se i dati abusivamente acquisiti da un server di posta elettronica vengono divulgati, si perfeziona il reato di cui all'art. 618 c.p.

Come si vede, la prevenzione dei reati informatici è particolarmente difficile e complessa, non solo per la stretta interconnessione fra tutti i possibili reati, ma soprattutto perché il limite di commissibilità è costituito unicamente dalla capacità e dalla competenza informatica di chi intende delinquere. A questo si aggiunga che nessun sistema è del tutto sicuro: esiste un livello accettabile di sicurezza che è definito dal bilanciamento di varie componenti, come il valore di quanto si intende difendere, l'investimento economico che si è disposti a sostenere, il livello di rischio che si è disposti a tollerare. Di certo non è pensabile prevedere un controllo rigido e capillare di tutte le attività che possono essere svolte per il tramite dell'utilizzo di attrezzature informatiche di un Ente: ciò, infatti, porterebbe sicuramente a paralizzarne del tutto l'attività. E', quindi, necessario addivenire ad un ragionevole compromesso fra tutte le esigenze in gioco, considerando che il fattore principale di tutte le attività di controllo è costituito dal livello etico e della professionalità degli addetti.

L'effettività dell'utilizzo dei protocolli penal-preventivi come condizione di riconoscibilità dell'esimente ex d.lgs. 231/01.

È pacifico in dottrina e in giurisprudenza che l'Ente, al fine di vedersi riconoscere l'esimente ex d.lgs. 231/01dalla responsabilità amministrativa da parte del Giudice per reati commessi da suoi apicali o dipendenti nel suo interesse o a suo vantaggio, deve aver formulato, adottato e fatto funzionare un Modello Organizzativo, Gestionale e di Controllo con finalità penal-preventive

rispondente ai criteri indicati dal d.lgs. 231/01. A tutto ciò si deve aggiungere la presenza, all'interno dell'Ente, e l'effettivo e continuo funzionamento di una struttura organizzativa permanente e specifica voluta dal d. lgs. 231/01, l'Organismo di Vigilanza, dotata degli strumenti e delle prerogative necessari per realizzare un continuo monitoraggio del rispetto, all'interno dell'Ente, di ogni singola componente del Modello Organizzativo, Gestionale e di Controllo nello svolgimento dell'attività propria della Società stessa.

L'Ente dunque, se vuole vedersi riconoscere dal Giudice l'esimente dalla responsabilità amministrativa ex d.lgs. 231/01, deve attivarsi effettivamente per poter dimostrare al Giudice di aver predisposto e attuato tutte le misure penal-preventive ritenute necessarie dal d. lgs. 231/01 e averle inserite nel Modello Organizzativo, Gestionale e di Controllo dall'Ente stesso predisposto, adottato ed effettivamente utilizzato. Tra queste misure rientrano sicuramente i protocolli adottati per prevenire la commissione dei reati informatici di cui all'art. 24 bis del d. lgs. 231/01 di cui si è detto in precedenza, compresi quindi controlli sull'attività lavorativa dei dipendenti, come anche degli apicali. Ma non solo: in effetti, a nostro giudizio, ogni componente del Modello Organizzativo, Gestionale e di Controllo deve recepire, nelle sue forme specifiche, misure penal-preventive verso tali reati.

La legittimità dei controlli: limiti e vincoli.

In materia di controlli a distanza, in mancanza di una disciplina legislativa specifica avente come oggetto la navigazione in Internet e poteri di controllo al riguardo in capo ai datori di lavoro, le normative alle quali si può fare riferimento sono due: il d.lgs 196/03 (Codice della Privacy) e la L.300/1970 (Statuto dei Lavoratori), in particolare gli artt. 4 (impianti audiovisivi) e 8 (divieto di indagini sulle opinioni). A disciplinare puntualmente la materia con specifiche pronunce e con provvedimenti mirati ha provveduto il Garante per la protezione dei dati personali, in particolare con il provvedimento intitolato "Linee-guida per posta elettronica e internet" del 1.3.2007. Infine di notevole interesse sono alcune pronunce giurisprudenziali, in particolare quelle che hanno definito le tipologie dei c.d. "controlli difensivi".

Il Codice della Privacy (d.lgs.196/03).

Il d.lgs. 196/03 disciplina il controllo a distanza in materia di trattamento dati personali richiamando espressamente gli artt. 4 e 8 dello Statuto dei Lavoratori. Agli artt. 113 e 114 si dispone, infatti, che, per quanto attiene alla raccolta dati e alla loro pertinenza (art.113) "resta fermo quanto disposto dall'art.8 della Legge 20.5.1970 n.300", così come, per quanto attiene ai controlli a distanza (art.114)" resta fermo quanto disposto dall'art.4 della Legge 20.5.1970 n. 300". Devono quindi essere rispettati sia il divieto di indagini sulle opinioni, disposto dall'art.8, sia la disciplina in materia di utilizzo di impianti audiovisivi contenuta nell'art. 4 dello Statuto dei Lavoratori. E' dunque il caso di richiamare brevemente i contenuti della disciplina dettata dallo Statuto dei Lavoratori.

Lo Statuto dei Lavoratori (L.20.5.1970 n.300)

Mentre l'art.8, vietando le indagini sulle opinioni dei lavoratori dipendenti, è rivolto a porre divieti sulle finalità del controllo a distanza come anche sul loro possibile esito, più diretto è quanto disposto dall'art.4, di cui vale la pena richiamare parte del testo. L'art.4 infatti, ai commi 1 e 2, recita:

"È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori. Gli impianti e le apparecchiature che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del Lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti".

Ci sembra indubbio che i controlli a distanza sull'utilizzo di strumenti informatici da parte di lavoratori dipendenti siano innanzitutto richiesti da esigenze organizzative, fra le quali possono ben rientrare le misure dell'Ente Collettivo conseguenti alla decisione di applicare al suo interno i dettami del d.lgs. 231/01 e, in particolare, i riflessi organizzativi del Modello Organizzativo, Gestionale e di Controllo con finalità penal-preventive, come l'effettuazione di controlli sulla navigazione in Internet e sull'utilizzo della posta elettronica da parte di lavoratori dipendenti, a meno che, come precisa l'art.4

comma 2, tali controlli siano stati oggetto di un accordo preventivo con le Organizzazioni Sindacali competenti, oppure, laddove un accordo non vi sia, siano stati autorizzati dall'Ispettorato del Lavoro. Tutto ciò attenua in modo netto il divieto di cui al comma 1, che, così come esplicitato, sembra assoluto. Pertanto l'Ente Collettivo, nell'adottare un Modello Organizzativo, Gestionale e di Controllo con finalità penal-preventive, ben può prevedere l'effettuazione di controlli sulle attività lavorative di dipendenti svolte mediante l'uso di strumenti informatici, e, in particolare, di posta elettronica e di Internet, a condizione che essa sia oggetto di accordo preventivo con le Organizzazioni Sindacali, ovvero di autorizzazione preventiva dell'Ispettorato del Lavoro.

Posta elettronica e Internet

Per quanto riguarda la posta elettronica il sistema più efficiente è quello dell'utilizzo, per i dipendenti, di un sistema di posta elettronica a mezzo WEB che renda inutile l'utilizzo dei sistemi impiegati per attività di lavoro. La Società può dunque vietare, nell'apposito disciplinare interno, l'uso della posta elettronica per motivi personali, avvertendo che procederà all'inoltro dei messaggi ad altri soggetti interni per evitare interruzioni nel flusso dei dati necessari all'attività di lavoro. Nel contempo potrà autorizzare l'uso di una casella di posta elettronica personale fornendo ogni utente di posta elettronica di una doppia casella, consentendo al firewall dell'Ente di accettare l'accesso al sito personale. Lo stesso principio può essere applicato a sistemi VoIP, chat o altro: in sostanza si procederà ad una netta differenziazione fra le attività professionali e quelle personali, destinando una parte del sistema informatico della Società ad usi personali, purché ben distinguibili dagli usi professionali.

I reati di cui all'art. 24-bis del decreto

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

Ai sensi dell'art. 615-ter c.p. "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

L'articolo offre una tutela ampia, comprensiva e anticipata che si sostanzia nel c.d. "ius excludendi alios", avente a oggetto tutti i dati raccolti nei sistemi informatici protetti, indipendentemente dal loro contenuto, purché attinenti alla sfera di pensiero o alle attività, lavorative e non, dell'utente, in modo da assicurare una protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-patrimoniali.

Per sistema informatico a mente della Convenzione di Budapest del 23 novembre 2001 si intende qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base a un programma, compiono l'elaborazione automatica dei dati.

Il delitto di cui all'art. 615-ter c.p. integra un reato di mera condotta che si perfeziona con la violazione del domicilio informatico, mediante l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi un'effettiva lesione della riservatezza degli utenti.

Le condotte punite dal primo comma consistono: a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (da intendere come accesso alla conoscenza

di dati o informazioni contenuti nel sistema, effettuato sia da lontano, sia da vicino); b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione (da intendersi come il fatto di chi persista nella già avvenuta introduzione, inizialmente autorizzata o casuale, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema).

Detenzione, diffusione e istallazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Ai sensi dell'art. 615-quater c.p. "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro. La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater".

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

A norma dell'art. 615-quinquies c.p. "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

L'articolo completa la normativa preventiva per assicurare il diritto dell'individuo di godere in modo indisturbato del proprio sistema, senza che lo stesso subisca danni illeciti. Gli strumenti cui fa riferimento la norma possono essere sia hardware, ad esempio smart card o pen drive USB, sia

software (nella maggior parte dei casi si tratterà di malware). Quest'ultimo termine deriva da "malicious software", generalmente conosciuto con il termine di virus.

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

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

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

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

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

La norma è indirizzata all'impedimento dell'intercettazione fraudolenta, che si verifica quando si prende conoscenza di comunicazioni altrui, in modo occulto e senza autorizzazione. Si tratta di una fattispecie a dolo generico e, salvo le aggravanti previste dal quarto comma, il reato è procedibile a querela della persona offesa.

In particolare, l'intercettazione si ha quando il messaggio giunge integralmente al destinatario, l'interruzione quando l'invio del messaggio viene interrotto e, pertanto, non giunge al destinatario, l'impedimento quando il messaggio non riesce nemmeno a partire.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

L'articolo dispone che: "Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater".

La norma offre una forma di tutela anticipata rispetto a quella prevista dall'art. 617-quater, punendo comportamenti prodromici alle condotte descritte nel precedente articolo. Per la realizzazione della fattispecie è sufficiente il mero pericolo di arrecare danno alla libertà di comunicare e alla riservatezza.

Le condotte consistono nella installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, a nulla rilevando l'effettivo funzionamento delle stesse.

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

Ai sensi della norma in commento "Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

La fattispecie si differenzia rispetto al danneggiamento ordinario per gli interessi tutelati inerenti la realtà informatica e telematica.

Le condotte sono rappresentante dalla distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi altrui.

La condotta della "cancellazione", secondo la giurisprudenza di legittimità, deve essere interpretata nella accezione informatica e non semantica del termine, ossia come la "rimozione da un

certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via 'definitiva' mediante il successivo svuotamento dello stesso". Pertanto, del tutto irrilevante, ai fini della sussistenza del reato, è il fatto che i file cancellati possano essere recuperati ex post attraverso una specifica procedura tecnico-informatica.

Secondo tale impostazione, la configurabilità del reato di danneggiamento informatico non viene dunque preclusa dall'eventuale reversibilità del danno, ritenendosi sufficiente che il bene tutelato sia stato - anche solo temporaneamente - oggetto di manomissione o alterazione rimediabile attraverso un postumo intervento riparatorio.

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

Ai sensi dell'art. 635-ter c.p. "Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma punisce i medesimi fatti sanzionati dall'art. 635 bis allorquando l'attività si diriga avverso informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità.

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

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

cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

La fattispecie richiama le condotte di cui all'art. 635-bis c.p. e punisce condotte ulteriori, quali l'introduzione o la trasmissione di dati, informazioni o programmi, che danneggino, distruggano, rendano anche in parte inservibili o ostacolino il funzionamento di altrui sistemi informatici o telematici.

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

Ai sensi della norma in commento: "Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

L'articolo punisce le condotte dell'art. 635 quater dirette a sistemi informatici o telematici di pubblica utilità.

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

L'articolo dispone: "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."

L'articolo tutela l'attività di rilascio di un certificato qualificato rispetto ad attività poste in essere dal certificatore che per fini ed interessi di tipo privato viola gli obblighi previsti dalla legge.

La fattispecie richiede il dolo specifico rappresentato dal fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

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

L'articolo prevede "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." Lo scopo della norma è la tutela della fede pubblica attraverso la salvaguardia dell'integrità del documento informatico nella sua valenza probatoria.

Trattamento sanzionatorio per le fattispecie di cui all'art. 24-bis del Decreto

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

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

Relativamente alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale (salvo quanto previsto dall'articolo 24 del Decreto per i casi di frode informatica in danno dello Stato o di altro Ente pubblico) si applica all'ente la sanzione pecuniaria sino a quattrocento quote. Nei casi di condanna per uno dei delitti indicati nel superiore n. 1) si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel superiore n. 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 superiore n. 3) si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

Le aree a rischio ed i presidi di controllo esistenti

Nel presente paragrafo, sono elencate le aree "a rischio reato" identificate nel corso della fase di risk assessment, con l'avvertenza che, per ciascuna area, sono altresì indicate:

- le cd. "attività sensibili", ovvero quelle nel cui ambito è effettivamente sussistente il rischio di commissione delle fattispecie delittuose, ed i reati astrattamente ipotizzabili;

- le funzioni aziendali coinvolte, fermo restando che in tutte le aree è ipotizzabile il coinvolgimento dell'amministratore unico, in quanto dotato di poteri gestionali e di rappresentanza sostanziale della Società;

- i controlli vigenti in seno alla Società, ovvero gli strumenti adottati al fine di mitigare il rischio di commissione dei reati.

Sotto tale ultimo profilo, occorre preliminarmente evidenziare che, in tutte le aree "a rischio reato" qui considerate, occorre osservare i seguenti Presidi di Controllo Generali (a cui si aggiungono Presidi di Controllo Specifici in relazione a singole attività sensibili o categorie di attività sensibili):

1) rispetto del Codice Etico;

2) formazione in ordine al Modello e alle tematiche di cui al D.Lgs. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;

3) diffusione del Modello tra le risorse aziendali, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi sulla intranet della Società;

4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito intranet della Società o messa a disposizione in formato cartaceo o telematico;

4) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari (ad es., fornitori, consulenti, appaltatori), si impegnano a rispettare le previsioni del Decreto;

5) previsione e attuazione del Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi;

6) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della Società, di impegno al rispetto dello stesso, incluso il Codice Etico;

7) implementazione di un sistema di dichiarazioni periodiche (almeno semestrali) da parte dei Responsabili Interni con le quali si fornisce evidenza del rispetto e/o della inosservanza del Modello (o, ancora di circostanze che possono influire sull'adeguatezza ed effettività del Modello); 8) creazione di una "Sezione 231" all'interno della intranet aziendale, presso cui pubblicare tutti i documenti

rilevanti nell'ambito del Modello della Società (ad es., Modello, Codice Etico, Protocolli aziendali in esso richiamati);

9) rispetto dell'organigramma aziendale;

10) rispetto di regole, procedure e istruzioni operative adottate dalla Società in tema di sicurezza informatica che riguardino, a titolo esemplificativo:

- uso accettabile delle risorse informatiche;
- controllo degli accessi alle risorse informatiche;
- gestione degli incidenti in materia di sicurezza delle informazioni e reazioni ai medesimi;
- sicurezza della rete e delle comunicazioni;

11) ogni altra documentazione relativa al sistema di controllo interno in essere nella Società.

Area a rischio n. 1: Processo tecnico / tutte le attività aziendali svolte tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso a Internet

Attività sensibili:

a) gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione;

b) evoluzione della piattaforma tecnologica e applicativa IT;

b) gestione dei flussi di comunicazione elettronici con Enti Pubblici;

c) utilizzo di software e di banche dati;

d) utilizzo di sistemi informatici di gestione e controllo degli adempimenti fiscali e amministrativi.

Reati ipotizzabili:

- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

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

- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) - danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

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

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

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

Ulteriori presidi (specifici) di controllo:

1) divieto posto a carico di tutti i destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato tra quelle sopra considerate;

- violare i principi di comportamento previsti nella presente Parte Speciale, nonché le regole e prassi aziendali di interesse;

2) individuazione e adozione di misure adeguate di sicurezza di natura organizzativa, fisica e logistica, in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o distruzione delle risorse informatiche e che si pongano quale obiettivo quello di:

- tutelare la sicurezza delle informazioni;

- prevedere eventuali controlli di sicurezza specifici per tipologia di asset;

- prevedere eventuali controlli di sicurezza destinati a indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali.

3) obbligo per tutti i destinatari del presente Modello di rispettare i principi comportamentali posti a presidio del rischio di commissione dei delitti informatici, volti ad assicurare l'osservanza dei seguenti parametri di sicurezza del patrimonio informativo della Società previsti dai principali standard internazionali in tema di sicurezza delle informazioni:

- riservatezza intesa come garanzia che una informazione sia accessibile solo a chi è autorizzato;

- integrità intesa come salvaguardia dell'accuratezza e della completezza dell'informazione e dei metodi di elaborazione;

- disponibilità intesa come garanzia che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse associate, quando richiesto.

In particolare, è vietato: (a) connettere ai sistemi informatici della Società personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;

(b) procedere a installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano il diritto d'autore;

(c) modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;

(d) acquisire, possedere, o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati, ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici;

(e) ottenere credenziali di accesso a sistemi informatici o telematici aziendali dei clienti o di terze parti con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;

(f) divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

(g) accedere abusivamente a un sistema informatico altrui – ovvero nella disponibilità di altri dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;

(h) manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

(i) sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

(l) acquisire e/o utilizzare prodotti tutelati dal diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;

(m) comunicare a persone non autorizzate, interne o esterne alla Società i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

(n) mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;

(o) lo spamming come pure ogni azione di risposta al medesimo; (p) inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;

(q) utilizzare per finalità diverse da quelle lavorative le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Società;

(r) alterare documenti elettronici, pubblici o privati, con finalità probatoria.

I destinatari del Modello sono tenuti a rispettare scrupolosamente tutte le norme vigenti, e in particolare:

• utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;

• custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;

• garantire la tracciabilità dei documenti prodotti;

• assicurare meccanismi di protezione dei file, quali, ad esempio, password da aggiornare periodicamente, secondo le prescrizioni comportamentali della Società;

• utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;

• utilizzare unicamente materiale pubblicitario (i.e. materiale fotografico) autorizzato.

4) informazione rivolta a tutti i destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi in ordine alla importanza di:

- mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
- utilizzare correttamente i software e banche dati in dotazione;
- non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;

5) formazione e addestramento periodico in favore dei dipendenti, diversificato in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore dei destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

6) sottoscrizione da parte dei dipendenti, nonché degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, di uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali; 7) informazione rivolta ai dipendenti e, in generale, a tutti i destinatari del Modello eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

8) limitazione degli accessi alle stanze server unicamente al personale autorizzato;

9) protezione, per quanto possibile, di ogni sistema informatico societario, al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative a un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

10) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venire disattivati;

11) impedire l'installazione e l'utilizzo di software non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;

12) informazione rivolta agli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore e in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

13) limitazione dell'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti a individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;

14) divieto di installazione e di utilizzo, sui sistemi informatici della Società, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, Virus, etc.) senza alcuna possibilità di controllo da parte della Società;

15) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, protezione degli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;

16) previsione di un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti, degli stagisti e degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi; 17) limitazione dell'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

18) cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;

19) nei rapporti contrattuali con i Fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, previsione di clausole di manleva volte a tenere indenne la

Società da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi;

20) Osservanza dei protocolli aziendali con particolare riguardo al Protocollo PRT07 lett. E relativo al Processo Tecnico (Sistema Informatico).

Area a rischio n. 2: amministrazione del personale

Attività sensibili:

1) installazione, manutenzione, aggiornamento e gestione di software di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti previdenziali ed assistenziali.

Reati ipotizzabili:

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

Area a rischio n. 3: gestione dei rapporti con l'amministrazione finanziaria

Attività sensibili:

a) Installazione, manutenzione, aggiornamento e gestione di software di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti fiscali.

Reati ipotizzabili:

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

Ulteriori presidi (specifici) di controllo: In relazione alle aree a rischio n. 2, 3:

1) rispetto dei ruoli, compiti e responsabilità definiti dall'organigramma nella gestione di sistemi, strumenti, documenti o dati informatici;

2) formale identificazione dei soggetti deputati alla gestione di sistemi, strumenti, documenti o dati informatici;

3) definizione delle modalità di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi;

4) rivisitazione periodica dei diritti d'accesso degli utenti;

5) accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati;

6) controlli formalizzati sugli accessi atti a presidiare il rischio di accesso non autorizzato alle informazioni, ai sistemi, alle reti e alle applicazioni, nonché atti a prevenire danni ed interferenze ai locali ed ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;

7) segregazione delle funzioni al fine di garantire operativamente la separazione del livello esecutivo da quello approvativo;

8) autenticazione individuale dell'utilizzo di dispositivi hardware e software dedicati per l'implementazione delle politiche di navigazione in internet e scambio delle informazioni (firewall, proxy server, ecc.);

9) meccanismi di protezione per lo scambio di informazioni tramite internet, posta elettronica e dispositivi rimovibili;

10) implementazione di misure di sicurezza atte a garantire l'accesso alle informazioni da parte di terze parti solo previa autorizzazione formale e nel rispetto degli accordi di riservatezza e confidenzialità stipulati;

11) implementazione di ambienti logicamente e fisicamente separati al fine di controllare e testare le modifiche software fino al rilascio in produzione;

12) definizione formale delle modalità di protezione da software pericolosi;

13) definizione formale delle modalità di gestione dei back-up delle informazioni e dei software;

14) formale classificazione delle informazioni e dei sistemi informatici gestiti dalla Società;

15) controlli formalizzati atti a presidiare il rischio di appropriazione e modifica indebita delle informazioni di proprietà della Società con conseguente perdita di autenticità, riservatezza ed integrità dell'asset informativo;

16) definizione delle modalità di custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, ecc.) e previsione di regole di clear screen per gli elaboratori utilizzati; 17) definizione delle tempistiche per la chiusura delle sessioni inattive;

18) formale definizione delle modalità operative per l'individuazione e la gestione degli incidenti e dei problemi;

19) verifica periodica di tutti gli incidenti singoli e ricorrenti al fine di individuarne le relative cause;

20) verifica periodica dei trend sugli incidenti e sui problemi al fine di individuare le azioni preventive al verificarsi di problemi in futuro;

21) valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi e che tenga conto della normativa applicabile in materia e dei principi etici della Società;

22) previsione di specifiche attività di formazione ed aggiornamenti periodici sulle procedure di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;

23) obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa per i dipendenti e per i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;

24) tracciabilità di tutte le operazioni effettuate per la gestione dei sistemi, strumenti, documenti o dati informatici utilizzati dalla Società.

I compiti dell'organismo di vigilanza

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i reati di cui all'art. 24-bis D. Lgs. 231/2001 sono i seguenti:

- svolgere verifiche sul rispetto della presente Parte Speciale e valutare la loro efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del D. Lgs. 231/2001. Con riferimento a tale punto l'OdV potrà proporre ai soggetti competenti della Società eventuali azioni migliorative o modifiche, qualora vengano rilevate violazioni significative delle norme sui delitti informatici, ovvero in occasione di mutamenti nell'organizzazione aziendale e nell'attività in relazione al progresso scientifico e tecnologico;

- proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale (tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico);

- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti l'OdV può accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti, nonché acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

In particolare, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici della presente Parte Speciale ovvero alle procedure aziendali attinenti alle aree sensibili sopra individuate.