MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Dlgs 231/2001

PARTE SPECIALE E

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Adottato dal Consiglio di Amministrazione del 04/11/2022

INDICE

1. DESTINATARI DELLA PARTE SPECIALE E

La presente Parte Speciale riguarda i comportamenti posti in essere da amministratori, dirigenti e dipendenti di Strada dei Parchi S.p.A. nonché dai suoi consulenti e partner in relazione al tipo di rapporto in essere con Strada dei Parchi S.p.A., coinvolti nei processi sensibili.

L'obiettivo della Parte Speciale E è che tutti i destinatari, come sopra individuati, adottino comportamenti conformi a prevenire la commissione dei reati informatici e trattamento illecito di dati previsti dall'art. 24-bis del D.Lgs. 231/01.

L'art. 24-bis del D.Lgs. 231/01 individua tre distinte categorie di reato la cui commissione contempla ipotesi di responsabilità a carico degli enti e in particolare:

- reati che comportano un accesso abusivo ad un sistema informatico o il danneggiamento ad un sistema informatico o ad informazioni, dati e programmi informatici, reati di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche, (art. 24-bis, comma 1);
- reati derivanti dalla detenzione o diffusione di codici di accesso a sistemi informatici o dalla detenzione o diffusione di apparecchiature, dispositivi o programmi atti al danneggiamento informatico o all'interruzione di un sistema informatico (art. 24-bis, comma 2);
- reati relativi al falso in documento informatico e frode informatica del soggetto che presta servizi di certificazione attraverso la firma digitale nonché reati connessi alla *cybersicurezza* nazionale di cui all'art. 1 comma 11 del D.L. n. 105/2019 (art. 24-bis, comma 3).

I reati contemplati al comma 1 dell'art. 24-bis (artt. 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies c.p.) sono caratterizzati dall'elemento comune della condotta di accesso abusivo, distruzione, deterioramento, cancellazione, alterazione o soppressione e si differenziano in relazione all'oggetto materiale ossia informazioni, dati o programmi informatici ovvero sistemi informatici e telematici.

I reati contemplati al comma 2 dell'art. 24-bis (artt. 615-quater e 615-quinquies c.p.) possono considerarsi accessori rispetto a quelli del comma 1 in quanto la detenzione o la diffusione di codici di accesso, di programmi o di dispositivi diretti a danneggiare o interrompere un sistema informatico, possono essere utilizzati per l'accesso abusivo ad un sistema o l'intercettazione di informazioni.

I reati contemplati al comma 3 dell'art. 24-bis riguardano, invece, gli utilizzi del mezzo elettronico finalizzati a minare la fede pubblica documentale ovvero la fiducia che la collettività ripone sulla veridicità o autenticità di un documento (art. 491-bis c.p.) o di una firma elettronica (art. 640-quinquies c.p.). Inoltre, con il D.L. n. 105/2019 art. 1 comma 11 sono state introdotte nuove fattispecie incriminatrici connesse alla *cybersicurezza* nazionale ora inserite al sopracitato comma 3 dell'art. 24-bis.

2. I DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato informatico e trattamento illecito di dati previste dal D.Lgs. 231/01, riportiamo qui di seguito una descrizione, in forma sintetica, dei reati alla cui commissione da parte di soggetti riconducibili alla Società è collegato il regime di responsabilità a carico della stessa.

I reati di seguito descritti sono stati introdotti con l'inserimento dell'art. 24-bis del D.Lgs. 231/01 ad opera dell'art. 7 della L. 18 marzo 2008 n. 48.

- art. 491-bis c.p. *(Falsità in un documento informatico pubblico avente efficacia probatoria)* Documenti informatici - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture

private.

- art. 615-ter c.p. *(Accesso abusivo ad un sistema informatico o telematico)*, la norma punisce chiunque si introduce abusivamente 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.
- art. 615-quater c.p. *(Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)*, la norma punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente riproduce, si procura, diffonde, comunica, installa 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.
- art. 615-quinquies c.p. *(Diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*, la norma punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, installa, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.
- art. 617-quater c.p. *(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)*, la norma punisce chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe o, ancora, rivela mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.
- 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)*, la norma punisce chiunque, fuori dai casi consentiti dalla legge, installa abusivamente apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
- art. 635-bis c.p. *(Danneggiamento di informazioni, dati e programmi informatici)*, la norma punisce chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.
- art. 635-ter c.p. *(Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)*, la norma punisce 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.
- art. 635-quater c.p. *(Danneggiamento di sistemi informatici o telematici)*, la norma punisce 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.
- art. 635-quinquies c.p. *(Danneggiamento di sistemi informatici o telematici di pubblica utilità)*, la norma punisce 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 di pubblica utilità o ne ostacola gravemente il funzionamento.
- art. 640-quinquies c.p. *(Frode informatica del certificatore di firma elettronica)*, la

norma punisce 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 alla legge per il rilascio di un certificato qualificato.

2.1. FALSITÀ IN DOCUMENTI INFORMATICI (art. 491-bis c.p.)

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (articoli da 476 a 493 c.p.), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico pubblico avente efficacia probatoria in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il concetto di "documento informatico" è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nella possibilità di attribuire allo stesso un'efficacia probatoria secondo le norme civilistiche.

Tra le fattispecie di reato previste e punite dal Codice Penale si richiamano, in particolare, i reati di falsità materiale o ideologica commessi da pubblico ufficiale o da privato, falsità in atti pubblici, falsità in certificati o autorizzazioni amministrative, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso, etc.

Il reato si configura anche per il soggetto che, pur non rivestendo le qualifiche richieste per la commissione dei reati propri, può commetterlo in concorso con il pubblico ufficiale o l'incaricato di un pubblico servizio.

Non sembrano, invece, trovare applicazione con riferimento ai documenti informatici le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.).

Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento (contraffazione) o quando il documento sia stato artefatto (alterazione), anche da parte dell'autore originario, mediante aggiunte e/o cancellazioni successive alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate ovvero quando è lo stesso autore del documento che attesta fatti non rispondenti al vero.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale può, ad esempio, compiersi mediante l'utilizzo di firma elettronica altrui.

Tra i reati richiamati dall'art. 491-bis, sono punibili a querela della persona offesa la falsità in scrittura privata (art. 485 c.p.) e, con riferimento a questa, l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.); il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Integra il delitto di falsità in documenti informatici, ad esempio, la condotta di chi falsifica documenti aziendali oggetto di flussi informatizzati o la condotta di chi altera informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una possibile attività ispettiva.

2.2. ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (art. 615-ter c.p.)

Il reato si realizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero quando vi si mantiene contro la volontà di chi ha diritto di escluderlo o, ancora, quando un soggetto, pur essendo entrato legittimamente in un sistema, lo utilizza per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema potendosi realizzare anche qualora lo scopo sia solo quello di dimostrare la propria abilità o

l'altrui vulnerabilità dei sistemi.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: il verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, ovvero dell'interruzione totale o parziale del suo funzionamento o, ancora, quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Società o anche di terzi concesse in licenza alla Società, mediante l'utilizzo di credenziali di altri colleghi abilitati.

Il delitto potrebbe, pertanto, essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi, per prendere cognizione di dati riservati altrui, o acceda abusivamente ai sistemi aziendali della Società per acquisire informazioni a cui non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della Società stessa.

L'accesso abusivo ad un sistema informatico o telematico si realizza anche nell'ipotesi in cui un soggetto, pur non effettuando alcuna sottrazione materiale di file, proceda alla stampa o alla copia di un documento contenuto nell'archivio del personal computer altrui ovvero alla visualizzazione dei suoi contenuti.

2.3. DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTI ALL' ACCESSO A SISTEMI INFORMATICI O TELEMATICI (art. 615-quater c.p.)

Il reato si realizza quando un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee a raggiungere tale scopo.

La fattispecie di reato, perseguibile d'ufficio, può considerarsi accessoria rispetto alla precedente in quanto intende reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso (codici, password, smart card, etc.) indipendentemente dalla messa in atto degli eventuali crimini informatici rispetto ai quali la condotta in parola risulta essere propedeutica.

L'ipotesi di reato si configura sia nel caso in cui il soggetto, in possesso legittimamente dei codici di accesso di cui sopra li comunica senza autorizzazione a terzi soggetti ovvero rilascia istruzioni o indicazioni che rendono possibile la ricostruzione dei codici di accesso e/o il superamento delle misure di sicurezza, sia nel caso in cui il soggetto se li procuri illecitamente.

Il delitto potrebbe, ad esempio, configurarsi qualora un dipendente della società "A" comunica ad un altro soggetto "B" la password di accesso alle caselle e-mail di un proprio collega "C", allo scopo di garantire a "B" la possibilità di controllare le attività svolte da "C", quando da ciò possa derivare un determinato vantaggio o interesse per la Società.

2.4. DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (art. 615-quinquies c.p.)

Il reato si realizza quando qualcuno, 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, abusivamente si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

La fattispecie di reato, perseguibile d'ufficio, intende reprimere anche la sola abusiva detenzione o diffusione di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli eventuali crimini informatici rispetto ai quali la condotta in parola risulta essere propedeutica.

L'ipotesi di reato richiede che il reo agisca a scopo di lucro o di altrui danno seppur nella valutazione della condotta potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di diffusione di programmi o di dispositivi da parte di chi, pur non essendo mosso da specifica finalità di lucro o di determinazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare eventi dannosi al sistema informatico o telematico.

Il delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della Società.

2.5. INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617-quater c.p.)

Il reato si realizza quando un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni o, ancora, rivela, parzialmente o integralmente, al pubblico il contenuto di tali comunicazioni mediante qualsiasi mezzo di informazione.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dalla Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore del sistema.

Durante la trasmissione di dati è possibile, mediante apposite tecniche di intercettazione, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei dati o comprometterne l'integrità o, ancora, ritardarne o impedirne l'arrivo a destinazione.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware), mentre l'impedimento o l'interruzione delle comunicazioni (c.d. "denial of service") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante l'impiego di virus informatici, ma anche mediante il sovraccarico del sistema con l'immissione di una mole rilevante di comunicazioni fittizie.

Il delitto potrebbe, ad esempio, configurarsi nel caso in cui con un vantaggio concreto per la Società, un dipendente impedisca una determinata comunicazione in via informatica o telematica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.

2.6. 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.)

Il reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, 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 o intercorrenti tra più sistemi.

La fattispecie di reato, perseguibile d'ufficio, può considerarsi accessoria rispetto alla precedente in quanto la condotta vietata è costituita dalla detenzione, diffusione e installazione di apparecchiature potenzialmente lesive a prescindere dalla circostanza che le stesse siano o meno utilizzate e che siano perpetrati gli eventuali crimini informatici rispetto ai quali la condotta in parola risulta essere propedeutica.

Il reato si integra, ad esempio, a vantaggio della Società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

2.7. DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (art. 635-bis c.p.)

Il reato si realizza quando un soggetto distrugge, deteriora, altera, elimina o cancella, in tutto o in parte, informazioni, dati o programmi altrui ivi inclusi, secondo un'interpretazione rigorosa, i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse con violenza alle persone o minaccia ovvero con abuso della qualità di operatore del sistema.

Il delitto potrebbe, ad esempio, configurarsi nel caso in cui con un vantaggio concreto per la Società, un dipendente elimini o alteri dei file o dei programmi informatici al fine di far venir meno la prova del credito da parte di un fornitore della Società ovvero di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

2.8. 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.)

Il reato si realizza quando un soggetto 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.

La fattispecie di reato si distingue dalla precedente in quanto, nel caso de quo, il danneggiamento ha ad oggetto informazioni, dati o programmi dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.

Il reato si integra anche nel caso in cui la condotta sia diretta a produrre gli eventi lesivi descritti in precedenza a prescindere dal prodursi in concreto del risultato ovvero del danneggiamento che, se si verifica, costituisce circostanza aggravante della pena.

Il delitto potrebbe, ad esempio, configurarsi nel caso in cui con un vantaggio concreto per la Società, un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso un ente pubblico e relativi ad un procedimento penale a carico della Società.

2.9. DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (art. 635-quater c.p.)

Il reato si realizza quando un soggetto mediante 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.

Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

Qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento di un sistema si integrerà, pertanto, il delitto di danneggiamento di sistemi informatici o telematici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p.

Il reato è perseguibile d'ufficio e sono previste aggravanti di pena se il fatto è commesso con violenza alle persone o minaccia o con abuso della qualità di operatore del sistema.

È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di informazioni, dati e programmi di cui sopra (art. 635-bis c.p.) qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il funzionamento.

Il delitto potrebbe, ad esempio, configurarsi nel caso in cui con un vantaggio concreto per la Società, un dipendente compia atti diretti a danneggiare i sistemi informatici o telematici di un'impresa concorrente o, anche, qualora ne ricorrano i presupposti, di un cliente.

2.10. DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (art. 635-quinquies c.p.)

Il reato si configura quando la condotta di cui all'articolo che precede è diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Il reato si configura anche se gli eventi lesivi non si realizzano in concreto costituendo il loro verificarsi circostanza aggravante della pena così come la commissione del fatto con violenza alle persone o minaccia ovvero con abuso della qualità di operatore del sistema.

Per la configurazione del reato i sistemi aggrediti debbono essere di pubblica utilità e, pertanto, se da un lato non è sufficiente l'utilizzo dei sistemi da parte degli enti pubblici in caso di impiego per fini diversi da quelli di pubblica utilità, dall'altro lato la norma può essere applicata anche al caso di sistemi utilizzati da privati ma per fini di pubblica utilità.

È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di informazioni, dati e programmi di cui sopra (art. 635-ter c.p.) qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il funzionamento.

In definitiva, nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui sopra (art. 635-ter c.p.), quel che rileva è, in primo luogo, che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

Il delitto potrebbe, ad esempio, configurarsi nel caso in cui con un vantaggio concreto per la Società, un dipendente compia atti diretti a danneggiare sistemi informatici o telematici di pubblica utilità aventi efficacia probatoria e relativi ad un procedimento penale a carico della Società.

2.11. FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA (art.640-quinquies c.p.)

Il reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Il reato è dunque un reato c.d. "proprio" in quanto può essere commesso solo da parte di un soggetto "certificatore qualificato" che esercita particolari funzioni di certificazione per la firma elettronica qualificata.

2.12 DELITTI PREVISTI ALL'ART. 1 COMMA 11 D.L. 105/2019

Con la legge di conversione del decreto legge 21 settembre 2019, n. 105, al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di interesse collettivo, il legislatore ha previsto l'istituzione del c.d. perimetro di sicurezza nazionale cibernetica (PSNC).
La nuova disciplina si applica alle amministrazioni pubbliche, agli enti e agli operatori nazionali da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione - anche parziali - ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. La nuova fattispecie incriminatrice prevede due condotte alternative,

una di tipo commissivo ed una di tipo omissivo, entrambe sorrette da un dolo specifico consistente nel fine di ostacolare o condizionare i procedimenti sopra descritti, ovvero le attività di ispezione e vigilanza. Quanto alla prima condotta, è punito chiunque fornisca informazioni, dati o elementi di fatto non rispondenti al vero rilevanti:

1. per la predisposizione o l'aggiornamento degli elenchi di cui all'art. 1, comma 2, lett. b), del Decreto legge;

2. per la predisposizione o l'aggiornamento dei comunicati di cui all'art. 1, comma 6, lett. a), del Decreto legge;

3. per lo svolgimento delle attività di ispezione e vigilanza della Presidenza del Consiglio dei Ministri e del Ministero dello Sviluppo Economico.

La condotta omissiva punisce, invece, chiunque ometta di comunicare tali informazioni, dati o elementi di fatto, entro il termine prescritto dal Decreto legge.

L'articolo 1, comma 11 del decreto legge 21 settembre 2019, n. 105 sopra richiamato prevede quanto segue:

"*Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, e' punito con la reclusione da uno a tre anni*".

3. PROCESSI SENSIBILI

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-bis del D.Lgs. 231/01.

La fattispecie di reato contemplata dall'art. 640-quinquies non è stata ritenuta significativa in quanto la "frode informatica nei servizi di certificazione di firma elettronica" può essere commessa solo da un "soggetto qualificato", la consumazione del reato all'interno della Società non è, pertanto, nemmeno astrattamente ipotizzabile.

Con riferimento, invece, alle ulteriori fattispecie di reato richiamate dall'art. 24-bis del D.Lgs. 231/01 è opportuno evidenziare che nell'ambito dell'ordinaria attività lavorativa vi è un diffuso utilizzo di strumenti informatici e, quindi, un'ampia possibilità di accesso ai relativi sistemi e dati.

Il rischio di commissione dei reati di cui alla presente Parte Speciale è stato, pertanto, valutato non circoscritto a specifiche aree di rischio, ma potendosi astrattamente realizzare in qualsiasi ambito di attività, ampiamente diffuso all'interno della Società.

Processi ed Attività Sensibili:

- Gestione dei sistemi informativi, con particolare riguardo (i) al rispetto delle misure di sicurezza previste affinché siano conformi alle prescrizioni del Regolamento UE 2016/679 ("**Regolamento GDPR**"), (ii) alla protezione dei dati dal rischio di intrusione o di utilizzo di terzi e (iii) alla verifica della presenza di codici d'accesso a software protetti dall'ingegno e di programmi suscettibili di recare danno;
- Tutte le attività aziendali svolte tramite l'utilizzo di sistemi informativi aziendali.

Settori Aziendali maggiormente interessati:

- Tutti i settori che, nelle loro attività, sono supportati da sistemi informativi.

4. PRINCIPI DI RIFERIMENTO GENERALI

4.1. IL SISTEMA ORGANIZZATIVO IN GENERALE

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- formale attribuzione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità;
- chiara descrizione delle linee di riporto;
- conoscibilità, trasparenza e pubblicità dei poteri e ruoli attribuiti;

Le procedure devono essere caratterizzate dai seguenti elementi:

- separazione all'interno di ciascun processo tra il soggetto che assume la decisione, il soggetto che esegue tale decisione ed il soggetto al quale è affidato il controllo del processo (c.d. segregazione delle funzioni);
- traccia scritta di ciascun passaggio rilevante del processo (c.d. tracciabilità);
- adeguato livello di formalizzazione.

4.2. IL SISTEMA DI DELEGHE E PROCURE

Il sistema di deleghe e procure societarie deve rispettare i seguenti requisiti essenziali:

- tutti coloro che intrattengono in nome e per conto di Strada dei Parchi S.p.A. rapporti verso l'esterno devono essere dotati di una procura e/o di una delega formale sempre rigorosamente aggiornata;
- l'ampiezza di ciascuna procura e/o delega va correlata alle responsabilità e ad un'adeguata posizione del procuratore / delegato nella struttura organizzativa aziendale;
- qualsiasi comportamento tenuto dal procuratore / delegato in violazione dei limiti assegnatigli o di altre disposizioni di legge o aziendali, con particolare riferimento ai comportamenti che possano fondatamente coinvolgere la Società nei reati di cui alla presente Parte Speciale, è causa di revoca immediata dei poteri conferiti.

4.3. PRINCIPI GENERALI DI COMPORTAMENTO

Gli amministratori, i dirigenti ed i dipendenti di Strada dei Parchi S.p.A., i consulenti e partner, sono tenuti, nella misura necessaria allo svolgimento delle attività di competenza, a osservare i seguenti principi generali:

- stretta osservanza delle leggi, dei regolamenti e delle procedure che disciplinano le attività aziendali con particolare riferimento alle attività a rischio per i reati informatici e trattamento illecito di dati;
- stretta osservanza delle regole definite dal Codice Etico, dal presente Modello, dalle procedure e norme di comportamento interne atte a prevenire e/o impedire la realizzazione di illeciti informatici da parte degli esponenti aziendali;
- conoscenza e rispetto della Procedura "Norme interne sulla Privacy" adottata da Strada dei Parchi S.p.A.;
- svolgimento delle attività sulla base di criteri di massima correttezza e trasparenza.

Conseguentemente, è vietato:

- 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, anche tentato, rientranti tra quelle richiamate dall'art. 24-bis del D.Lgs. 231/01;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé

fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o favorirne la commissione;

- violare le regole contenute nelle procedure e, in generale, nella documentazione adottata in attuazione dei principi di riferimento previsti nella presente parte speciale;
- violare le regole in materia di trattamento dei dati personali;
- violare i principi previsti nel Codice Etico;
- porre in essere qualsiasi situazione il cui scopo si rivolga o si risolva essenzialmente nel danneggiamento di informazioni, dati o programmi informatici ovvero di sistemi informatici o telematici;
- porre in essere qualsiasi situazione il cui scopo si rivolga o si risolva essenzialmente nella falsificazione di un documento informatico.

È fatto, in generale, divieto di:

- tentare o porre in essere azioni o comportamenti riconducibili alle fattispecie di reato richiamate al capitolo 2;

ovvero, in particolare:

- alterare documenti informatici aventi efficacia probatoria al fine, ad esempio, di:
  - formare - ovvero concorrere a formare con un pubblico ufficiale o incaricato di pubblico servizio - documenti informatici falsi;
  - contraffare o alterare - ovvero concorrere a contraffare o alterare con un pubblico ufficiale o incaricato di pubblico servizio - documenti informatici veri;
  - contraffare o alterare - ovvero concorrere a contraffare o alterare con un pubblico ufficiale o incaricato di pubblico servizio – certificati o autorizzazioni amministrative contenute in un documento informatico ovvero le condizioni richieste per la loro validità;
  - formare - ovvero concorrere a formare con un pubblico ufficiale o incaricato di pubblico servizio – una copia su documento informatico di un atto pubblico o privato inesistente ovvero una copia diversa dall'originale;
  - contraffare - ovvero concorrere a contraffare con un pubblico ufficiale o incaricato di pubblico servizio – un attestato;
  - concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare in un documento informatico una falsa attestazione da parte di quest'ultimo che è un fatto è stato da lui compiuto o avvenuto alla sua presenza;
  - concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare in un documento informatico una falsa attestazione da parte di quest'ultimo che una dichiarazione non resa sia da lui stata ricevuta o che dichiarazioni da lui ricevute siano omesse o alterate;
  - concorrere con esercenti la professione sanitaria o forense o altro servizio di pubblica necessità a attestare falsamente sotto forma di documento informatico fatti per i quali il documento stesso è destinato a provare la verità;
  - attestare falsamente sotto forma di documento informatico in un atto pubblico o verso un pubblico ufficiale fatti per i quali il documento stesso è destinato a provare la verità;
  - scrivere o lasciar scrivere falsamente su documenti o database informatici dati ed indicazioni soggette ad ispezione dell'autorità giudiziaria;
  - scrivere o lasciar scrivere sotto forma di documento informatico notificazioni dirette all'autorità giudiziaria con false indicazioni su operazioni industriali,

commerciali o professionali;

- formare sotto forma di documento informatico scritture private, in tutto o in parte, false o alterare scritture private vere, utilizzandole o lasciando che altri le utilizzino;
- scrivere o far scrivere su un documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino;
- scrivere o far scrivere - ovvero concorrere a scrivere o a far scrivere con un pubblico ufficiale o incaricato di pubblico servizio – su un documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello cui il pubblico ufficiale o incaricato di pubblico servizio era obbligato o autorizzato;
- distruggere, sopprimere, occultare, in tutto o in parte, una scrittura privata o un atto pubblico veri e disponibili sotto forma di documento informatico;
- utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo;

- accedere abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero permanere nel sistema contro la volontà espressa o tacita di chi ha il diritto di escluderlo al fine, ad esempio, di:
  - acquisire informazioni mirate allo spionaggio industriale;
  - acquisire informazioni facenti capo a concorrenti, potenziali clienti ovvero enti detentori di dati di interesse mirate allo sviluppo di un'offerta commerciale o di una nuova iniziativa;
  - alterare dati e informazioni relativi alla Società che sono detenuti da banche o pubbliche amministrazioni;
  - alterare dati e informazioni che, relativi ad una commessa ultimata o in corso di esecuzione da parte della Società, sono detenuti dal cliente;
  - alterare informazioni contenute nei sistemi informatici aziendali allo scopo, ad esempio, di manipolare i dati destinati a confluire nel bilancio della Società;
- acquisire, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo;
- acquisire, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero di interrompere totalmente o parzialmente o alterare il suo funzionamento;
- intercettare, impedire o interrompere comunicazioni informatiche o telematiche ovvero diffondere al pubblico il contenuto, totale o parziale, di tali comunicazioni mediante un qualsiasi mezzo di informazione al fine, ad esempio, di:
  - intercettare fraudolentemente comunicazioni di concorrenti nell'ambito della partecipazione ad una gara d'appalto o di fornitura svolta su base elettronica al fine di falsarne o conoscerne preventivamente l'esito;
  - impedire o interrompere comunicazioni di concorrenti allo scopo, ad esempio, di ostacolare l'invio della documentazione d'offerta per la partecipazione ad una gara d'appalto o di altro materiale allo scopo, ad esempio, di determinare un'inadempienza del concorrente nei riguardi del cliente;

- installare apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero comunicazioni intercorrenti tra più sistemi;
- distruggere, danneggiare, rendere totalmente o parzialmente inservibili sistemi informatici o telematici, ovvero programmi, informazioni o dati altrui al fine, ad esempio, di:
  - impedire o danneggiare l'attività di un concorrente;
- distruggere, danneggiare, rendere totalmente o parzialmente inservibili sistemi informatici o telematici, ovvero programmi, informazioni o dati di pubblica utilità al fine, ad esempio, di:
  - impedire l'attività di un ente di vigilanza o di controllo ovvero comprometterne l'efficacia;
  - impedire l'attività dell'autorità giudiziaria ovvero comprometterne l'efficacia.

5. PRINCIPI DI RIFERIMENTO PER I REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

L'attuazione delle regole e dei divieti elencati nel precedente capitolo richiede - con riferimento alle singole attività sensibili individuate all'interno di Strada dei Parchi S.p.A. - l'adozione di specifici protocolli aziendali che definiscano gli standard a cui le Direzioni e le aree organizzative di Strada dei Parchi S.p.A. devono, per quanto di loro competenza, conformarsi nello svolgimento delle attività aziendali.

Facendo salvo il rigoroso rispetto del Codice Etico, delle procedure e norme aziendali, di seguito sono descritti i protocolli adottati da Strada dei Parchi S.p.A. al fine di prevenire le fattispecie di reato di cui alla presente Parte Speciale.

Tra le procedure e norme aziendali, si richiamano, in particolare, le Norme interne sulla Privacy e il Documento di Utilizzo degli Strumenti Informatici Aziendali in cui sono analizzati i sistemi informativi della Società e sono definite le procedure poste a garanzia della sicurezza dei dati personali con particolare riferimento a:

- i server;
- le misure di sicurezza per il trattamento informatico dei dati;
- gli strumenti antivirus;
- i sistemi anti-intrusione;
- i firewall;
- i piani di disaster recovery.

Al fine di assicurare i presidi necessari a prevenire le fattispecie di reato, anche tentato, rientranti tra quelle richiamate dall'art. 24-bis del D.Lgs. 231/01, sono definiti i seguenti protocolli che gli amministratori, i dirigenti ed i dipendenti della Società, i consulenti e i partner, nonché gli ulteriori soggetti eventualmente autorizzati nell'ambito delle attività a rischio, sono chiamati a rispettare:

- formare adeguatamente i dipendenti nonché gli stagisti e gli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi, sull'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi e sulla necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli con i codici di accesso in caso di allontanamento dalla postazione di lavoro;
- rispettare le misure specifiche per la sicurezza delle informazioni e tutela dei dati in materia di protezione dei dati personali (D.Lgs. 196/2003), così come adeguate dal D.Lgs. n. 101/2018 al Regolamento GDPR;

- utilizzare le informazioni, i dati, i programmi e i sistemi informatici esclusivamente per le attività attinenti alla propria mansione ovvero ai compiti assegnati;
- astenersi dall'utilizzare le apparecchiature informatiche in dotazione al di fuori delle autorizzazioni prescritte;
- non prestare o cedere a terzi apparecchiature informatiche aziendali senza la preventiva autorizzazione del responsabile dei sistemi informatici;
- in caso di smarrimento o furto di apparecchiature informatiche aziendali, presentare immediata denuncia all'autorità giudiziaria preposta e informare tempestivamente il responsabile dei sistemi informatici ovvero il proprio responsabile;
- utilizzare la connessione a internet esclusivamente per lo svolgimento delle proprie mansioni ovvero dei compiti assegnati e per il tempo strettamente necessario;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio personal computer ovvero consentire l'utilizzo dello stesso ad altre personale (familiari, amici, etc.);
- evitare l'utilizzo di password di altri utenti aziendali e l'accesso ad aree protette in nome e per conto di essi, salvo espressa autorizzazione del responsabile dei sistemi informatici ovvero del proprio responsabile;
- informare immediatamente il responsabile dei sistemi informatici qualora si venga a conoscenza della password di un altro utente;
- astenersi dal divulgare, cedere o condividere con altri le proprie credenziali di accesso ai sistemi informatici della Società, ovvero ai sistemi informatici di clienti, partner o enti terzi;
- astenersi dall'ottenere credenziali di accesso ai sistemi informatici della Società, ovvero dei sistemi informatici di clienti, partner o enti terzi, con metodi o procedure differenti da quelle autorizzate allo scopo;
- astenersi dal comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi aziendali e le modalità con cui gli stessi sono utilizzati;
- astenersi dallo sfruttare eventuali "buchi" nelle misure di sicurezza dei sistemi informatici aziendali, ovvero dei sistemi informatici di clienti, partner o enti terzi, per ottenere l'accesso a risorse o informazioni diverse da quelle per le quali si è autorizzati ad accedere, e ciò anche nel caso in cui l'intrusione non provochi danni a archivi, documenti e programmi informatici;
- astenersi dal modificare la configurazione hardware e/o software delle postazioni di lavoro fisse o mobili senza preventiva autorizzazione del responsabile dei sistemi informatici;
- astenersi dall'utilizzare strumenti hardware e/o software che potrebbero essere adoperati abusivamente per compromettere la sicurezza di sistemi informatici o telematici ovvero per intercettare comunicazioni informatiche;
- astenersi dal falsificare, alterare o eliminare il patrimonio informatico aziendale, ovvero il patrimonio informatico di clienti, partner o enti terzi, ivi compresi archivi, documenti o programmi informatici;
- evitare di introdurre e/o conservare nei sistemi informatici della Società, a qualsiasi titolo e per qualsiasi ragione, materiale informatico di proprietà di terzi, salvo che lo stesso sia stato acquisito con il loro espresso consenso o da loro trasmesso;
- evitare di introdurre e/o conservare nei sistemi informatici della Società, a qualsiasi titolo e per qualsiasi ragione, applicazioni informatiche di dubbia provenienza o che non siano state preventivamente approvate dal responsabile dei sistemi informatici;
- evitare di trasferire all'esterno della Società e/o trasmettere documentazione riservata

di proprietà della Società o qualsiasi altro file se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio responsabile;

- astenersi dall'effettuare copie non specificamente autorizzate su supporto informatico di archivi, documenti e programmi;
- astenersi dallo spamming come pure da ogni azione di risposta allo stesso;
- astenersi dall'installare programmi che non siano stati preventivamente autorizzati dal responsabile dei sistemi informatici;
- segnalare senza indugio utilizzi e/o funzionamenti anomali dei sistemi informatici al responsabile dei sistemi informatici;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici.

Oltre ai suddetti specifici comportamenti sono, inoltre, posti in essere dalla Società i seguenti ulteriori protocolli generali per la gestione del patrimonio informatico aziendale:

- sono individuate — nel rispetto del principio della separazione dei ruoli — le strutture aziendali preposte alla gestione della sicurezza dei dati e delle informazioni, nonché alla gestione delle infrastrutture di rete e dei sistemi e sono attribuiti alle medesime specifici compiti in materia di prevenzione dei delitti informatici e di trattamento illeciti di dati;
- vengono monitorati, affinché la gestione della sicurezza dei sistemi informativi sia adeguata e corretta, i log di accesso ai sistemi aziendali da parte della funzione sistemi e servizi per reti viarie ed i Log ai singoli applicativi da parte dei responsabili degli applicativi stessi, come individuati nel registro gestione del patrimonio software. Ciò al fine di individuare tempestivamente sia l'esistenza di attività che potrebbero determinare il mancato rispetto delle regole aziendali sia l'esistenza di accessi e dispositivi non autorizzati;
- sono predisposti strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici attraverso, in particolare: l'uso indebito o non autorizzato della password; la detenzione o installazione di software non previsto dalle procedure aziendali, ivi compresi virus e spyware di ogni genere e natura e dispositivi atti all'interruzione di servizi o alle intercettazioni; l'accesso a siti protetti ovvero non visitabili; il collegamento non consentito di hardware alla rete aziendale. Tali misure prevedono regole in merito; alle restrizioni all'accesso fisico ai luoghi in cui sono collocati i sistemi centrali (CED); l'attribuzione e revoca della password, tenendo conto delle mansioni aziendali per le quali viene richiesta/concessa; alla rimozione dei diritti di accesso al termine del rapporto di lavoro; il controllo e la tracciabilità degli accessi; le modalità di svolgimento delle attività di gestione e manutenzione dei sistemi; la previsione di controlli sulla idoneità della rete aziendale e sul suo corretto instradamento (routing); l'esistenza di procedure di controllo della installazione di software sui sistemi operativi o sui terminali aziendali;
- sono adottate specifiche misure di protezione volte a garantire l'integrità delle informazioni messe a disposizione del pubblico tramite la rete internet;
- sono adottate specifiche misure di protezione e mappatura dei documenti elettronici utilizzati per comunicazioni verso l'esterno;
- sono adottate specifiche misure a garanzie che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale, avvenga in conformità a disposizioni di legge o contrattuali;

- sono adottati specifici strumenti per la individuazione, prevenzione e ripristino dei sistemi rispetto a virus e altre vulnerabilità;
- è attuato un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente e le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati;
- è implementato un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici;
- è svolta una attività di analisi degli eventi registrati volta a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce;
- previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti;
- predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni);
- predisposizione e attuazione dì una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive;
- inventariare le attrezzature hardware, i programmi software e le licenze d'uso;
- sottoporre l'inventario e l'effettiva dotazione, in programmi e attrezzature, a periodici sistematici controlli;
- conservare i programmi software in luoghi idonei alla loro salvaguardia;
- prevedere, per ciascun profilo aziendale o dipendente, delle password di accesso personalizzate in funzione dei ruoli e dei compiti attribuiti agli utilizzatori dei sistemi informatici e telematici;
- affidare la gestione delle password di accesso ad un'unica funzione responsabile del sistema di attribuzione e modifica periodica;
- affidare la gestione dell'amministrazione e configurazione dei personal computer ad un'unica funzione responsabile dei sistemi informatici;
- conservare le password di accesso ai sistemi informatici e telematici in luoghi protetti;
- registrare gli accessi a internet e alle reti telematiche e monitorare la trasmissione e diffusione di dati;
- eseguire periodiche e sistematiche attività di:
  - verifica sulle dotazioni hardware e software e sul possesso delle previste licenze;
  - verifica su eventuali utilizzi illegittimi dell'hardware e/o del software;
  - verifica della possibilità di cracking delle password;
  - verifica della possibilità di accesso a programmi e reti senza l'utilizzo di password;
  - verifica della possibilità di duplicazione di opere protette dal diritto d'autore ovvero di rimozione delle informazioni elettroniche sul regime dei diritti;
- informare periodicamente l'O.d.V. sugli aspetti rilevanti afferenti a:
  - la dotazione di hardware, software e licenze d'uso;
  - l'utilizzo delle attrezzature e dei programmi e dei sistemi informatici e telematici;
- segnalare all'O.d.V. sugli aspetti rilevanti afferenti a:

- le deroghe alle procedure interne decise per rispondere a particolari esigenze;
- i presunti o accertati delitti informatici o trattamento illecito di dati.

6. I CONTROLLI DELL'O.d.V.

Fermo restando il potere discrezionale dell'O.d.V. di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'O.d.V. effettua periodicamente controlli a campione sulle attività connesse ai processi sensibili ai reati informatici diretti a verificare la loro corretta esecuzione in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere.

Per l'effettuazione di tali controlli periodici, l'O.d.V. si avvale, altresì, della collaborazione delle altre funzioni aziendali.

Inoltre, a titolo esemplificativo, alcune delle attività di verifica sulla presente Parte Speciale che l'O.d.V. può svolgere sono le seguenti:

- Svolgere verifiche periodiche 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'O.d.V. – avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia – potrà condurre una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà 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 sensibili 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.

Si ribadisce che all'O.d.V. viene garantita la libertà di accesso a tutte attività aziendali e la disponibilità di consultazione e/o acquisizione di tutta la documentazione rilevante.

7. TESTO DELL'ART. 24-BIS DEL D.LGS. 231/2001

Art. 24-Bis
Delitti informatici e trattamento illecito di dati (1)
* * *

1. *In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies terzo comma (2), del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
2. *In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*
3. *In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto 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, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*
4. *Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).*

(1) Articolo aggiunto dall'articolo 7 della legge 18 marzo 2008, n. 48.

(2) Il presente comma era stato modificato dall'art 9, co. II, D.L. n. 93 del 14.08.2013, tuttavia, detta modifica, non è stata confermata dalla legge di conversione n. 119 del 15.10.2013.