Modello di Organizzazione, Gestione e Controllo

Versione 1.0 del 13 aprile 2021

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

In particolare, il titolare della Privacy deve verificare il corretto impiego dei sistemi informatici, delle procedure e chiavi di accesso ed in generale verificare l'assenza di elementi ostativi dettati dalle norme della presente parte speciale.
Inoltre, deve essere verificata l'attendibilità commerciale e professionale dei fornitori e manutentori di software e programmi aziendali.

Dovrà inoltre essere garantita:

- la formazione/informazione del personale;
- la professionalità ed affidabilità degli amministratori di sistema;
- il controllo costante degli interventi effettuati e del rispetto delle misure di sicurezza adottate dalla società.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione dei dati, informazioni e documenti informatici (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano ricostruibili le autorizzazioni all'uso e le responsabilità in materia di codici di accesso, chiavi elettroniche, password e misure di sicurezza in genere;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- siano effettuati i necessari controlli sull'integrità di dati, informazioni e documenti informatici;
- sia impedita la divulgazione e l'appropriazione abusiva di codici di accesso, chiavi elettroniche, password e misure di sicurezza in genere;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione informatica da parte degli organi a ciò deputati;
- siano effettuate con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalle procedure interne, dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale ed adeguate all'evoluzione della tecnologia; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PROCEDURA AREA TECNICA

1. Il Piano di Sicurezza Informatica

1.1. Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dall'Accademia per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati. Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs 196/2003, "Codice in materia di protezione dei dati personali" e del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza". Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo dell'Accademia un adeguato livello di sicurezza.

1.2. Obbiettivi

Scopo del presente documento è descrivere la strategia che l'Accademia intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- *Confidenzialità*: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.
- *Integrità*: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).

- *Disponibilità*: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.
- *Accountability (Tracciabilità)*: tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento. Il Piano per la sicurezza informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice dell'Accademia.

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

1.3. Responsabilità (figure coinvolte)

L'Ente predispone il Piano per la sicurezza informatica ai sensi dell'art.12 del DPCM 13 novembre 2014. Tale piano risulta essere comprensivo del Piano per la sicurezza informatica dei documenti di cui all'art. 4 del DPCM 3 dicembre 2013, relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, predisposto dal Responsabile della gestione documentale nel rispetto del D.Lgs 196/2003 e del relativo Allegato B, d'intesa con il Responsabile del trattamento dei dati personali.

2. Il Sistema Informativo dell'Accademia

2.1. Tipologia di servizi offerti

Il Sistema Informativo dell'Accademia è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze "interne" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza della popolazione residente esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi strettamente Accademici, oppure tramite un sistema esterno, reso disponibile da altri enti e all'Accademia stessa accessibile con le opportune modalità.

2.2. Servizio Informativo

2.2.1. Organizzazione

Nel contesto del Sistema Informativo ogni utente dell'Accademia deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia di Utenti	Compiti/Responsabilità	Note
Addetti Assistenza Informatica Esterna	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, ecc.). Verifiche sull'attuazione delle politiche.	
Dipendenti della Segreteria	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati.	Si faccia riferimento al mansionario specifico.
Responsabili	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati. Vigilanza sul comportamento dei dipendenti e degli addetti esterni.	Si faccia riferimento ad Organigramma
Amministratore di Rete Amministratore di Sistema	Verifica su attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche. Verifica su politiche di sicurezza informatiche, fisiche e sociali. Reporting e certificazione regolari sullo stato della struttura	Andrea Gianfreda

2.2.2. Addetti

Nel contesto del Sistema Informativo ogni dipendente dell'Accademia è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto

concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica è incaricata una figura interna con la consulenza di una società esterna specializzata in tale settore, la quale svolge anche attività di assistenza hardware e software.

2.3. Infrastruttura Tecnologica

2.3.1. Generalità

L'Infrastruttura Tecnologica dell'Accademia può essere schematizzata come segue:

Tipologia di Apparati	Descrizione
Apparati Server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà dell'Accademia o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso il locale CED del distaccamento di Via Cefalonia 58 – Brescia (BS).
Apparati Server esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società esterne o da Enti esterni (MIUR, etc), in virtù di contratti stipulati con l'Accademia.
Apparati di rete	Indichiamo in questa categoria tutti gli apparati (router, switch, hub, …) che concorrono alla connettività fra le sedi dell'Accademia (connettività interna), da e verso Internet (connettività pubblica verso l'esterno).
Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli apparati che concorrono specificatamente alla sicurezza (storage per backup, apparati firewall).
Infrastruttura di comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano, per ogni sede, la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet.
Apparati client	In questa categoria raggruppiamo tutti gli apparati (PC, Portatili, …) utilizzati dall'utenza interna per l'utilizzo dalle sedi territoriali o in connettività mobile dei servizi dell'Accademia

2.3.2. Struttura Fisica

Il sistema informatico dell'Accademia è così costituito:

- Server SRV-DC1 - Windows Server 2019 – con funzioni di Domain Controller Primario
- Server SRV-DC2 - Windows Server 2019 – con funzioni di Domain Controller di Backup
- Server SHARE - Windows Server 2019 – con funzioni di File Server
- Server Gestionale – Windows Server 2012 – con funzioni di service provider per l'uso del gestionale interno e deposito della relativa banca dati
- Server Business – Windows Server 2019 – con funzione di service provider per l'uso del gestionale Amministrativo e deposito della relativa banca dati
- Server Management – Windows Server 2016 – con funzioni di management dei precedenti
- NAS di rete utilizzato come unità di storage per tutti i dati cartacei relativi alla didattica (come dispense, programmi ecc.)
- NAS di rete utilizzato come unità di backup per il precedente
- Server "Microsoft" esterno utilizzato per la gestione del dominio, del servizio di posta elettronica e di una serie di applicazioni rivolte al personale interno.

Nel locale CED situato nel distaccamento di Via Cefalonia sono presenti le macchine fisiche:

- Dell PowerEdge R640 – 10 x Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz – 64GB RAM -1TB HDD – 256GB SSD
- Dell PowerEdge R430 – 8 x Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz – 48GB RAM - 3TB HDD
- Dell – Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz – 16GB RAM - 2TB HDD

Le sedi dell'Accademia sono poi dotate di due connettività al fine di garantire la navigazione Extranet ed Intranet dei loro utenti. Le connessioni ricadono sotto le seguenti categorie:

- FTTH (Fiber To The Home) 100: rappresenta la connettività backbone dedicata alle VPN, alla navigazione e in generale ogni operazione svolta dagli uffici.
- FFTC (Fiber To The Cabinet) 100/20: rappresenta la connettività di riserva dedicata principalmente alla navigazione degli studenti e dei docenti.

2.3.3. Architettura Applicativa

Nel presente paragrafo descriviamo i principali software applicativi ed utilità in uso presso l'Accademia esplicitandone le caratteristiche salienti. Dal punto di vista della architettura applicativa possiamo distinguere le seguenti categorie:

- Software centralizzati: trattasi di applicativi in uso a livello di Accademia, installati in unica posizione, su server presso la sede, o in uno degli ambienti virtuali disponibili, oppure resi disponibili da enti esterni e usufruibili dall'Accademia via Web. Quasi sempre la architettura elaborativa è a 3 livelli, composta da un database server, da un

application (e web) server con accesso dei client via Web tramite la Intranet ed Extranet dell'Accademia.
- Software stand-alone: in questa categoria intendiamo software installati localmente sulle postazioni di lavoro, essenzialmente ai fini della produttività personale.

2.3.4. Sistema di Conservazione

I dati trattati dall'Accademia sono salvati e protetti come indicato nell'apposita sezione del GDPR Aziendale. Le tipologie di dati possono essere così riassunte:

- Dati Anagrafici e Accademici: le informazioni anagrafiche dei soggetti che transitano in LABA, così come le informazioni relative alla loro carriera Accademica, vengono salvate all'interno di un Database SQL interrogato dal software Gestionale interno.
- Dati Economico-Amministrativi: le informazioni di carattere economico-amministrativo, come dati anagrafici, coordinate bancarie, situazione contabile ecc. degli studenti e dei fornitori LABA sono salvate all'interno di un Database SQL interrogato dal software Business Cube.
- Le mail istituzionali di studenti, docenti e personale interno e avanti dominio laba.edu, vengono interamente gestite dai server esterni di Microsoft Office 365.
- Il materiale realizzato dagli studenti (e raccolto dai Docenti durante l'anno accademico) viene salvato e conservato nell'archivio OneDrive di un account istituzionale dedicato.
- Le registrazioni delle lezioni vengono salvate, se d'accordo con il Docente relatore, nell'account Steam del registrante o all'interno del canale relativo alla materia del Docente stesso.

3. Politiche Organizzative della Sicurezza

3.1. Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno dell'Accademia richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo. L'applicazione delle politiche di sicurezza all'interno dell'Accademia richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.

Attualmente, l'individuazione della politica di sicurezza determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1. Backup

I dati, in qualunque modo elaborati dai sistemi informatici dell'Accademia, sono salvati nella memoria centrale del Server Microsoft Windows 2019. Al fine di salvaguardarne l'integrità è stato attivato un sistema di duplicazione e memorizzazione giornaliero dei dati informatici che effettua il backup delle macchine virtuali ove sono salvati tali dati. Per ridurre ancor più la probabilità di eventuali disservizi il piano di disaster recovery prevede che questa copia abbia carattere ridondante e venga distribuita sui due NAS di rete a disposizione; ad oggi non è pianificato un backup dei dati in Cloud ma non se ne esclude la possibilità di una prossima implementazione.

3.2. Sicurezza Logica

3.2.1. Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi, in modo tale da garantirne la fruibilità nel tempo, che deve essere al contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2. Sistema di Autenticazione

La credenziale di autenticazione consiste in un indirizzo e-mail atto all'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo.

Le credenziali di autenticazione sono affidate al controllo del Server Microsoft Windows 2019 che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di Microsoft Active Directory ("insieme di servizi di rete - account utente, account computer, cartelle condivise, stampanti, etc. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei client") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione).

Tramite tecnologia SSO (Single Sign-On) tali credenziali verranno poi utilizzate per unificare gli accessi degli utenti ai vari servizi messi a disposizione dell'Accademia come la navigazione wi-fi all'interno degli spazi condivisi, l'ingresso ai servizi Microsoft O365 e al nuovo gestionale di prossima implementazione.

Ad integrare la protezione sul sistema informativo, i software dell'Accademia e gli applicativi web sono dotati di apposite procedure di accesso tramite username ("nome con il quale l'utente viene riconosciuto da un computer, da un programma o da un server") e password ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo username è un identificativo che, insieme alla password, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.3. Antivirus e Similari

Il sistema informatico dell'Accademia e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-quinquies del Codice Penale ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"), mediante l'attivazione:

- ***software antivirus*** stand-alone installato sui singoli elaboratori. La posta elettronica è invece protetta mediante l'antivirus integrato nel Server di posta elettronica di Microsoft O365 ("software atto a rilevare ed eliminare virus informatici o altri programmi dannosi");
- ***software antispyware*** installato sui singoli elaboratori ("programma il cui scopo è quello di cercare ed eliminare dal sistema, tramite un'apposita scansione, i software che raccolgono informazioni riguardanti l'attività on-line di un utente - siti visitati, acquisti eseguiti in rete etc. - senza il suo consenso per farne un uso illegittimo");
- ***software antispam*** integrato nel Server di posta elettronica di Microsoft O365 ("software che individua messaggi di posta elettronica indesiderati generalmente commerciali e/o pubblicitari").

I sistemi operativi degli elaboratori e dei Server sono periodicamente aggiornati automaticamente mediante Windows Update con le opportune patch di sicurezza ("programma o parte di programma che aggiorna e corregge un software"). Regolarmente e costantemente il Responsabile aggiorna, vigila e controlla.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

Al fine di prevenire intrusioni dall'esterno è stato installato e configurato un firewall hardware e su ciascun elaboratore è stato attivato il firewall software integrato nel sistema operativo "Microsoft Windows". Periodicamente sono stati eseguiti e verranno effettuati, nei tempi previsti dalla normativa, gli aggiornamenti sui sistemi di protezione.

4. Documenti e Banche Dati

4.1. Sistema di Gestione Informatica dei Documenti

Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti". Tale sistema è attivato dall'Istituto su tutte le postazioni di lavoro degli uffici afferenti all'AOO e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili individuati all'interno dell'AOO (Responsabile della gestione documentale, Responsabile dei sistemi informativi).

Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'Accademia si faccia riferimento alle indicazioni contenute nel GDPR Aziendale, così come anche per i seguenti argomenti:

- Protocollo informatico
- Formazione dei documenti
- Formati adottati
- Sottoscrizioni
- Validazione temporale
- Metadati
- Trasmissione dei documenti
- Conservazione

5. Trattamento dei Dati Personali – Analisi e Gestione dei Rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando al GDPR Aziendale.

5.1. Gestione dei Rischi

Al fine di minimizzare i rischi di corruzione, perdita, alterazione, furto dei dati, l'Istituto adotta le seguenti politiche di sicurezza.

5.1.1. Configurazione dei Sistemi

I sistemi in utilizzo sulla rete sono installati in configurazioni standard con software di comprovata stabilità e sicurezza. Il personale dipendente dell'Accademia è informato sui rischi dovuti all'installazione e all'utilizzo di software non conformi alle politiche di sicurezza o quantomeno non sufficientemente testati. Il Responsabile che materialmente esegue le installazioni dei sistemi provvede a disattivare tutti i servizi non necessari e a chiudere le porte TCP/UDP non necessarie al corretto funzionamento degli applicativi.

5.1.2. Sicurezza

L'Amministratore di rete certifica di essere:

- abbonato a servizi offline/online in materia di sicurezza informatica e a servizi offline/online di alert in materia di cyberattacchi, sicurezza informatica, virus
- in possesso delle certificazioni che gli consentono di operare sui software applicativi in uso nella rete LAN senza invalidarne le garanzie dei produttori

PARTE SPECIALE

“H”

Violazione del diritto d’autore

L'articolo 15, c. 7, della legge 23 luglio 2009 n. 99, recante "*Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*", ha introdotto l'articolo 25 *novies*, rubricato "Delitti in materia di violazione del diritto d'autore".

Si tratta, in particolare, dei seguenti reati:

Art. 171 legge 633/1941 – Messa a disposizione del pubblico, in un sistema di reti telematiche, di un'opera dell'ingegno protetta o di parte di essa.

Comma 1 lett. a) *bis*
Salvo quanto previsto dall'art. 171-bis e dall'art. 171-ter, è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
omissis
a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

Comma 3
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

****

Art. 171-*bis* legge 633/1941

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

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

****

Considerazioni specifiche

Il bene giuridico protetto riguarda gli interessi patrimoniali dei titolari del diritto di sfruttamento economico del *software*. Costituisce reato la condotta di abusiva duplicazione di programmi anche in assenza di una finalità di natura patrimoniale. È configurabile il reato di cui alla norma ogniqualvolta i programmi informatici illegalmente detenuti abbiano concretamente favorito l'attività imprenditoriale esercitata dall'autore del fatto, venendo impiegati per attività funzionali all'impresa, come l'archiviazione dei dati relativi ai fornitori o ai clienti, l'elencazione delle scadenze contabili o la gestione delle fatturazioni. L'indicazione del comportamento vietato viene operata dall'articolo facendo riferimento ai vari diritti di utilizzazione economica dell'opera dell'ingegno.

Art. 171-*ter* legge 633/1941

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a

disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti commessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

****

Art. 171-*septies* legge 633/1941

La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

****

Art. 171-*octies* legge 633/1941

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove,

installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

****

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** ogni settore della Società dove vengono impiegati strumenti informatici (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano in generale l'utilizzo del sistema informatico.
Il rischio, in questo caso, potrebbe essere rappresentato dall'utilizzo abusivo di programmi informatici, anche per uso endo aziendale, senza acquisto della relativa licenza.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono:

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le

norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.

- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.
- I Destinatari interessati devono inoltre assicurarsi che nei contratti di acquisto di prodotti interessati da un diritto di proprietà industriale altrui sia prevista la licenza di utilizzo di tali diritti di proprietà industriale.

Dovrà inoltre essere garantita:

- la formazione specifica del personale delle aree interessate in materia di proprietà industriale, mirata a rendere consapevoli i destinatari riguardo ai problemi giuridici connessi alla gestione dei relativi diritti;
- la definizione di regole relative alla promozione dei prodotti ed ai rapporti con i concorrenti ed i clienti;
- la sensibilizzazione degli esponenti aziendali circa il corretto utilizzo delle risorse aziendali altrui in tema di proprietà industriale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono:

A. attuare un controllo preventivo e continuativo delle attività connesse con, o che implicano, l'utilizzo di diritti di proprietà industriale di terzi;
B. effettuare i necessari controlli sui contratti di cessione o licenza di diritti di proprietà industriale di terzi nonché sui procedimenti e/o i prodotti su cui esiste un diritto di proprietà industriale di terzi;
C. mantenere una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
D. segnalare tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolare ogni forma di controllo da parte di quest'ultimo;
E. garantire la costante formazione ed aggiornamento del personale dipendente e dei collaboratori esterni (agenti, collaboratori, ecc.) che operano nelle aree aziendali a rischio per i reati di cui alla presente parte speciale;

F. non porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione informatica da parte degli organi a ciò deputati;
G. effettuare con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalle procedure interne, dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"I"

Reati di criminalità organizzata

L'articolo 2, comma 29, della legge 15 luglio 2009 n. 94, recante "*Disposizioni in materia di sicurezza pubblica*", ha introdotto nel Decreto l'articolo 24-*ter*, rubricato "Delitti in materia di criminalità organizzata".

Si tratta, in particolare, dei seguenti reati:

Art. 416, 6° comma - Associazione per delinquere

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602*, nonché all'*articolo 12, *comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al* decreto legislativo 25 luglio 1998, n. 286, *si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.*

Art. 416-*bis* del codice penale – Associazione di tipo mafioso

Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni.

Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma.

L'associazione si considera armata quanto i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.

Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

**articolo così modificato dall'articolo 5 della legge 69 del 27 maggio 2015.*

****

Considerazioni specifiche

Come già evidenziato nella predetta parte speciale, attraverso lo strumento del reato associativo vi è il concreto rischio che alcune fattispecie illecite finora escluse dal novero di quelle considerate dal Decreto possano rientrare in questo ambito.

Art. 416-*ter* del codice penale - Scambio elettorale politico-mafioso

La pena stabilita dal primo comma dell'articolo 416-bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416-bis in cambio della erogazione di denaro.

****

Considerazioni specifiche

Vista l'attività della Società, si tratta di reato ben difficilmente configurabile in seno alla stessa.

Art. 630 del codice penale - Sequestro di persona a scopo di rapina o di estorsione

Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da venticinque a trenta anni.

Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta.

Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.

Al concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà, senza che tale risultato sia conseguenza del prezzo della liberazione, si applicano le pene previste dall'articolo 605. Se tuttavia il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da sei a quindici anni.

Nei confronti del concorrente che, dissociandosi dagli altri, si adopera, al di fuori del caso previsto dal comma precedente, per evitare che l'attività delittuosa sia portata a conseguenze ulteriori ovvero aiuta concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di prove decisive per l'individuazione o la cattura dei concorrenti, la pena dell'ergastolo è sostituita da quella della reclusione da dodici a venti anni e le altre pene sono diminuite da un terzo a due terzi.

Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma.

I limiti di pena preveduti nel comma precedente possono essere superati allorché ricorrono le circostanze attenuanti di cui al quinto comma del presente articolo

Considerazioni specifiche

Si tratta di reato ben difficilmente configurabile in seno alla Società.

Art. 74 DPR 9 ottobre 1990, n. 309 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope.

Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 70, commi 4, 6 e 10, escluse le operazioni relative alle sostanze di cui alla categoria III dell'allegato I al regolamento (CE) n. 273/2004 e dell'allegato al regolamento n. 111/2005, ovvero dall'articolo 73, chi promuove, costituisce, dirige, organizza o finanzia l'associazione è punito per ciò solo con la reclusione non inferiore a venti anni.

Chi partecipa all'associazione è punito con la reclusione non inferiore a dieci anni.

La pena è aumentata se il numero degli associati è di dieci o più o se tra i partecipanti vi sono persone dedite all'uso di sostanze stupefacenti o psicotrope.

Se l'associazione è armata la pena, nei casi indicati dai commi 1 e 3, non può essere inferiore a ventiquattro anni di reclusione e, nel caso previsto dal comma 2, a dodici anni di reclusione. L'associazione si considera armata quando i partecipanti hanno la disponibilità di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

La pena è aumentata se ricorre la circostanza di cui alla lettera e) del comma 1 dell'articolo 80.

Se l'associazione è costituita per commettere i fatti descritti dal comma 5 dell'articolo 73, si applicano il primo e il secondo comma dell'articolo 416 del codice penale.

Le pene previste dai commi da 1 a 6 sono diminuite dalla metà a due terzi per chi si sia efficacemente adoperato per assicurare le prove del reato o per sottrarre all'associazione risorse decisive per la commissione dei delitti.

Quando in leggi e decreti è richiamato il reato previsto dall'articolo 75 della legge 22 dicembre 1975, n. 685, abrogato dall'articolo 38, comma 1, della legge 26 giugno 1990, n. 162, il richiamo si intende riferito al presente articolo.

****

Considerazioni specifiche

Si tratta di reato ben difficilmente configurabile in seno alla Società, presupponendo, come è stato sottolineato dalla giurisprudenza, la presenza di tre elementi fondamentali: *(I)* l'esistenza di un gruppo, i membri del quale siano aggregati consapevolmente per il compimento di una serie indeterminata di reati in materia di stupefacenti; *(II)* l'organizzazione di attività personali e di beni economici per il perseguimento del fine illecito comune, con l'assunzione dell'impegno di apportarli anche in futuro per attuare il piano permanente criminoso; *(III)* sotto il profilo soggettivo, l'apporto individuale apprezzabile e non episodico di almeno tre associati, che integri un contributo alla stabilità dell'unione illecita.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come aree "a rischio" ogni settore della Società (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano, in generale, la gestione delle attività sensibili riportate nell'analisi dei rischi per le quali sono previste ipotesi di reato qualificabili come delitti in forma associativa.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.
Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono assicurarsi che:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;

- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia garantito, anche da parte dei subappaltatori e dei terzi in genere che espletino servizi o producano beni per conto della Società, il rispetto della normativa vigente in materia di immigrazione e di lavoro, ivi incluso per ciò che attiene al profilo della costituzione del rapporto lavorativo;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non giustificati in relazione al tipo di incarico effettuato ed alla prassi ed alle eventuali tariffe vigenti;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati;
- siano effettuate con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.
Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello az

PARTE SPECIALE

"L"

Delitti di impiego di lavoratori stranieri irregolari

L'articolo 2 del D.lgs. 16 luglio 2012, n. 109 (recante "*Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare*") ha introdotto nel Decreto l'articolo 25-*duodecies*, rubricato "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*". Si tratta delle ipotesi aggravanti del reato di cui all'articolo 12 del D.lgs. 286/1998, relativo all'impiego di lavoratori stranieri irregolari, ipotesi aggravanti che ricorrono:

- se i lavoratori occupati sono in numero superiore a tre;
- se i minori occupati sono minori in età non lavorativa;
- se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-*bis* del codice penale.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** le seguenti aree:

A. Consiglio di Amministrazione
B. Ufficio personale (relativamente all'individuazione e selezione dei lavoratori ed alla stipula dei successivi contratti nonché alla gestione del rapporto di lavoro).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale sono:

i) selezione ed assunzione di personale;
j) verifica iniziale e periodica della documentazione di lavoratori stranieri (regolare possesso e validità da parte del lavoratore straniero di regolare permesso di soggiorno);
k) implementazione delle procedure autorizzative connesse al rapporto di lavoro.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.

- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

In particolare, l'Ufficio personale deve selezionare ed assumere esclusivamente personale in regola con la normativa in materia di immigrazione e deve altresì controllare la regolarità della documentazione presentata dai dipendenti e collaboratori da assumere, con particolare riferimento al possesso di un regolare e valido permesso di soggiorno.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.

Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"M"

Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali

L'articolo 25-quater del D. Lgs. 231/2001 non richiama specificatamente una serie di reati, bensì fa un generico riferimento ai "Delitti con finalità di terrorismo o di eversione dell'ordine democratico" previsti dal codice penale e dalle leggi speciali, nonché all'articolo 2 della Convenzione Internazionale del terrorismo fatta a New York il 9 dicembre 1999.

Di seguito quanto riportato dall' art. 2 della Convenzione Internazionale:

1. Commette reato ai sensi della presente Convenzione ogni persona che, con qualsiasi mezzo, direttamente o indirettamente, illecitamente e deliberatamente fornisce o raccoglie fondi nell'intento di vederli utilizzati, o sapendo che saranno utilizzati, in tutto o in parte, al fine di commettere: a) un atto che costituisce reato ai sensi e secondo la definizione di uno dei trattati enumerati nell'allegato; b) ogni altro atto destinato ad uccidere o a ferire gravemente un civile o ogni altra persona che non partecipa direttamente alle ostilità in una situazione di conflitto armato quando, per sua natura o contesto, tale atto sia finalizzato ad intimidire una popolazione o a costringere un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere, un atto qualsiasi.
3. Affinché un atto costituisca reato ai sensi del paragrafo 1, non occorre che i fondi siano stati effettivamente utilizzati per commettere un reato di cui ai commi a) o b) del paragrafo 1 del presente articolo.
4. Commette altresì reato chiunque tenti di commettere reato ai sensi del paragrafo 1 del presente articolo.
I trattati richiamati dall'articolo sono numerosi e fanno riferimento a diverse convenzioni internazionali aventi l'obiettivo di reprimere gli atti di terrorismo. (A titolo esemplificativo si riportano: Protocollo per la repressione di atti illeciti diretti contro la sicurezza delle installazioni fisse sulla piattaforma continentale - Roma, 10 marzo 1988, Convenzione internazionale per la repressione degli attentati terroristici con esplosivo, adottata dall'Assemblea generale delle Nazioni Unite il 15 dicembre 1997, ecc.).

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio**" le seguenti aree:

C. Consiglio di Amministrazione
D. Direzione amministrativa
E. Ufficio personale

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale sono :

- Procedure di assunzione : selezione/assunzione personale, verifica preliminare sui requisiti del candidato.

- Procedure di gestione utenza : corretto adempimento degli obblighi in materia di antiterrorismo previsti dalla normativa vigente.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- La Società garantisce la conformità dell'operatività alle disposizioni vigenti in materia di antiterrorismo/antiriciclaggio, avvalendosi di specifici applicativi in grado di consultare le basi dati dei nominativi sospetti di finanziamento al terrorismo.
- Gli uffici preposti, in conformità alle vigenti prescrizioni di legge ed al ruolo rivestito nei rapporti con i fornitori e/o clienti, approntano e consultano le liste antiterrorismo predisposte dagli organismi ufficiali.

- La Società garantisce controlli automatici sui nominativi sospetti di terrorismo e provenienti da Paesi con cui è vietato dalla normativa operare (Black List).
- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.
In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.
Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"N"

Delitti contro la personalità individuale

L'art. 5 della Legge 11 agosto 2003, n. 228 ha introdotto, nel corpo del D. Lgs. 231/2001 (di seguito, 'Decreto'), l'art. 25-quinquies, il quale prevede la responsabilità degli enti per i delitti contro la personalità individuale, commessi dai propri soggetti apicali o subordinati nell'interesse e/o vantaggio della società stessa. Segnatamente, l'articolo in questione prevede:

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

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

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

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

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

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

Di seguito vengono riportate la fattispecie incriminatrici richiamate dal Decreto.

Riduzione o mantenimento in schiavitù o in servitù (art. 600, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque eserciti su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduca o mantenga una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento. La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta venga attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Prostituzione minorile (art. 600 bis, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque recluti o induca alla prostituzione una persona di età inferiore agli anni diciotto oppure ne favorisca, sfrutti, gestisca, organizzi e controlli la prostituzione ovvero altrimenti ne tragga profitto. Tale norma sanziona, inoltre, chiunque compia atti sessuali con un minore di età

compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi.

Pornografia minorile (art. 600 ter, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, sfruttando minori di anni diciotto, realizzi esibizioni o spettacoli pornografici o produca materiale pornografico ovvero chiunque recluti o induca minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli ne tragga altrimenti profitto. La fattispecie punisce anche chiunque faccia commercio del materiale pornografico e chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisca, divulghi o pubblicizzi il materiale pornografico di cui al primo comma, ovvero distribuisca o divulghi notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto; ovvero chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente ceda ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto. Infine, tale norma sanziona chiunque assista a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto.

Detenzione di materiale pornografico (art. 600 quater, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, al di fuori delle ipotesi previste nell'articolo 600 ter, cod. pen., consapevolmente si procuri o disponga di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto.

Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque organizzi o propagandi viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività.

Tratta di persone (art. 601, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque commetta tratta di persona che si trova nelle condizioni di cui all’articolo 600, cod. pen., ovvero, al fine di commettere i delitti di cui al medesimo articolo, la induca mediante inganno o la costringa mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno. 5

Acquisto e alienazione di schiavi (art. 602, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, fuori dei casi indicati nell'articolo 601, cod. pen., acquisti o alieni o ceda una persona che si trova in una delle condizioni di cui all'articolo 600, cod. pen. Per quanto attiene ai reati sopra considerati, va tenuto presente che possono essere ritenuti responsabili degli stessi non solo i soggetti che direttamente realizzino le fattispecie criminose, ma anche i soggetti che consapevolmente agevolino, anche solo finanziariamente, la medesima condotta. Di conseguenza, potrebbero rientrare nell'ipotesi di reato sopra considerate, le eventuali erogazioni di risorse economiche in favore di soggetti terzi, effettuate da parte dell'Ente con la consapevolezza che le erogazioni stesse possano essere utilizzate da tali soggetti per finalità criminose

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** ogni settore della Società (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano l'utilizzo del sistema informatico (es. rischio di download da siti web classificati come pericolosi e non attinenti all'attività lavorativa aziendale; salvataggio su pc aziendali di materiale pornografico tramite memorie esterne come pen drive).

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita

evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.

- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- Siano utilizzati strumenti informatici costantemente aggiornati ed elaborati da reputate imprese del settore che impediscano l'accesso e/o ricezione di materiale relativo alla pornografia minorile (strumenti di "content filtering");
- Nel rispetto delle normative vigenti, siano svolti periodici controlli volti ad impedire l'abuso dei sistemi informativi aziendali o la commissione di reati attraverso il loro utilizzo;
- Siano effettuati richiami netti e inequivocabili volti al corretto uso degli strumenti informatici in possesso dei dipendenti;
- Sia svolta una attenta valutazione di possibili partnership commerciali con società operanti in settori quali la comunicazione telematica di materiale relativo alla pornografia minorile e il turismo nelle aree geografiche richiamate al punto precedente;
- Siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- Siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- Sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- Siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;

- Non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.
In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.

Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.