Parte Speciale 6

I DELITTI INFORMATICI ed I DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

LIVORNO FERRARIS

STORICO DELLE MODIFICHE		
Rev.	Natura della modifica	
0	Prima stesura	
1	Aggiornamento	
APPROVAZIONE		
Rev.		Data
1	Approvato dal Consiglio di Amministrazione	26/07/2017
2	Approvato dal Consiglio di Amministrazione del	21/12/2018
3	Approvato dal Consiglio di Amministrazione del	16/06/2020

Di seguito vengono elencati i reati previsti rispettivamente dall'art. 24 bis (delitti informatici e trattamento illecito di dati) e dell'art. 25 novies (delitti in violazione del diritto d'autore).

FATTISPECIE DI REATO	SANZIONI PREVISTE DAL D.LGS. 231/01
I DELITTI INFORMATICI PREVISTI DALL'ART. 24bis D.Lgs. 231/01 **Art. 615 ter c.p.** - Accesso abusivo ad un sistema informatico o telematico **Art. 615 quater c.p**. - Detenzione e diffusione abusiva di codici di accesso **Art. 615 quinquies c.p.** - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) **Art. 617 quater c.p.-** Intercettazione, impedimento o interruzione illecita di comunicazioni) **Art. 617 quinquies c.p.** - Installazione di apparecchiature atte ad intercettare comunicazioni) **Art. 635 bis c.p.** - Danneggiamento di informazioni, dati e programmi informatici **Art. 635 ter c.p.** - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato **Art. 635 quater c.p.** - Danneggiamento di sistemi informatici o telematici **Art. 635 quinquies c.p.** - Danneggiamento di sistemi informatici o telematici di pubblica utilità **Art. 640 quinquies c.p.** - Frode informatica del soggetto che presta servizi	Per i delitti di cui agli artt. 615 ter – 617 quater – 617 quinquies – 635 bis – 635 ter – 635 quater e 635 quinquies: ▪ sanzione pecuniaria da 100 a 500 quote ▪ sanzioni interdittive: interdizione dall'esercizio dell'attività – sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito – divieto di pubblicizzare beni o servizi, per una durata non inferiore a tre mesi e non superiore a due anni. Per i delitti di cui agli artt. 615 quater e 615 quinquies: ▪ sanzione pecuniaria sino a 300 quote; ▪ sanzioni interdittive: sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito – divieto di pubblicizzare beni o servizi, per una durata non inferiore a tre mesi e non superiore a due anni. Per i delitti di cui agli artt. 491 bis e 640 quinquies e Art. 1 Decreto Legge 21 settembre 2019, n. 105 convertito in Legge con modifiche dalla Legge 18 novembre 2019, n. 133: ▪ sanzione pecuniaria sino a 400 quote; sanzioni interdittive: divieto di contrattare con la PA –

di certificazione di firma elettronica **Art. 491 bis c.p.** - documenti informatici **Articolo 1 Decreto legge 21 settembre 2019, n. 105 convertito in legge con modifiche dalla legge 18 novembre 2019, n. 133 -** Perimetro di sicurezza nazionale cibernetica. In merito si è in attesa dell'atto amministrativo del Presidente del Consiglio dei Ministri che su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), individui i soggetti tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo. A ciascuno dei soggetti inseriti nell'elenco verrà data pronta comunicazione. Qualora la Società dov'esse ricevere tale comunicazione, sarà quindi necessario procedere ad un approfondimento in merito.	esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi – divieto di pubblicizzare beni o servizi, per una durata non inferiore a tre mesi e non superiore a due anni.
I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE PREVISTI DALL'ART. 25 NOVIES del D.Lgs. 231/01 **Artt. 171, primo comma lett. a bis) e terzo comma della L. n. 633/1941** **Art. 171 bis della L. n. 633/1941** **Art. 171 ter della L. n. 633/1941** **Art. 171 septies della L. n. 633/1941** **Art. 171 octies della L. n. 633/1941**	▪ Sanzione pecuniaria fino a 500 quote ▪ Sanzioni interdittive per una durata non superiore ad un anno

ATTIVITA'/PROCESSO A RISCHIO	PRINCIPALI FUNZIONI/SOGGETTI COINVOLTI	LIVELLO DI RISCHIO
GESTIONE DEL SISTEMA INFORMATICO **GESTIONE ACQUISTI PROGRAMMI SOFTWARE** **GESTIONE ACCESSO AD INTERNET**	▪ Presidente CdA ▪ Tutti i dipendenti, dirigenti, amministratori e comunque tutti coloro che hanno accesso alla rete informatica aziendale ▪ Consulenti e collaboratori esterni coinvolti nella gestione delle attività sensibili **Funzioni centrali di governo e di gestione fornite in service da EPP:** ▪ CFO ▪ Procurement ▪ Legal & Corporate Affairs ▪ Information and Communication Technology	BASSO

I DESTINATARI

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dirigenti, dipendenti della Società, nonché dai Collaboratori esterni e Partner e compresi gli eventuali soggetti appartenenti ad EP Produzione Spa (anche semplicemente "EPP") coinvolti nella gestione delle aree di attività a rischio.

La presente parte speciale prevede, quindi, che nell'espletamento delle rispettive attività, i soggetti coinvolti nelle predette attività sensibili, siano tenuti al rispetto dei principi di comportamento e delle procedure che regolamentano tale area a rischio.

PRINCIPI DI COMPORTAMENTO PREVENTIVI

I PRINCIPI GENERALI DI COMPORTAMENTO

La presente parte speciale prevede che nell'espletamento delle rispettive attività, i soggetti coinvolti nelle predette attività sensibili, compresi collaboratori esterni, siano tenuti, al fine di prevenire e impedire il verificarsi dei reati previsti dagli artt. 24 bis e 25 novies del D. Lgs. 231/01, al rispetto dei seguenti principi di comportamento.

La presente parte speciale prevede l'**espresso divieto** a carico dei destinatari di :

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra indicate;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra indicate, possano potenzialmente diventarlo.

E' inoltre sancito **l'espresso obbligo** di:

- tenere comportamenti in linea con i principi espressi nel Codice Etico e nel presente Modello Organizzativo;
- rispettare tutte le norme di legge applicabili e le procedure interne adottate;
- inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a

conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla Società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali);

- monitorare periodicamente i programmi software utilizzati ed il numero delle licenze in possesso.

I PRINCIPI SPECIFICI DI COMPORTAMENTO

Oltre ai principi generali sopra descritti che devono sempre trovare applicazione nella gestione di tutte le attività e di tutti i processi c.d. a rischio, la presente parte speciale indica, anche una serie di ulteriori principi specifici di prevenzione che tutti i soggetti coinvolti devono rispettare, al fine di prevenire e impedire il verificarsi dei predetti reati.

In merito ai reati di cui all'art. 25 novies, è vietato:

- scaricare tramite un programma di file sharing software protetti dal diritto d'autore o files contenenti musica, film o e immetterli a disposizione del pubblico;
- mettere 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;
- duplicare programmi per elaboratore o importare o software protetti dal diritto d'autore, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori e editori (SIAE);
- pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico o far fa ascoltare in pubblico duplicazioni o riproduzioni abusive, con fine di lucro;
- violare licenze, diritti d'autore e le leggi e regolamenti locali, nazionali ed internazionali che tutelano la proprietà intellettuale e le attività on-line.

In merito ai reati di cui all'art. 24 bis, è vietato:

- falsificare, in tutto o in parte, un documento informatico avente efficacia probatoria o alterarne uno vero;
- alterare o contraffare un documento informatico con particolare riferimento a procedure amministrative, come certificati o autorizzazioni;
- inserire dati o informazioni non veritiere quando queste sono destinate ad elaborazioni informatizzate o elenchi o registri elettronici;
- installare, scaricare e/o utilizzare programmi informatici che permettano di alterare, contraffare, attestare falsamente, sopprimere, distruggere e/o occultare documenti informatici pubblici o privati o che consentano l'introduzione abusiva all'interno di sistemi informatici o telematici protetti da misure di sicurezza o che permettano la permanenza (senza averne l'autorizzazione) al loro interno, in

violazione delle misure poste a presidio degli stessi dal titolare dei dati o dei programmi che si intende custodire o mantenere riservati;
- reperire, diffondere, condividere e/o comunicare passwords, chiavi di accesso, o altri mezzi idonei a permettere l'accesso ad un sistema informatico protetto da misure di sicurezza;
- accedere abusivamente a sistemi informatici;
- diffondere codici di accesso a sistemi informatici, telematici;
- danneggiare dati o sistemi informatici di pubblica utilità o meno.

Nell'utilizzo delle tecnologie è obbligatorio:
- attenersi scrupolosamente alle modalità e ai criteri stabiliti per l'assegnazione, gestione e utilizzo delle misure di sicurezza su tutti i computer in uso, nonché su portatili, smartphone e tablet aziendali in dotazione;
- osservare e rispettare le disposizioni vigenti per il rilascio di un certificato qualificato di firma elettronica;
- osservare attentamente le regole e le procedure adottate per la gestione in sicurezza dei sistemi informatici e/o telematici anche ai fini della tutela del diritto d'autore di eventuali programmi, software e banche dati soggetti a copyright.

PRESIDI PREVENTIVI ADOTTATI

Per ciò che concerne le citate aree di rischio e le relative attività sensibili, EPCLF ha predisposto una serie di misure preventive, specifiche e concrete. Tra queste, a mero titolo esemplificativo e non esaustivo, si menzionano:

- la diffusione del Codice Etico e del Modello Organizzativo e rispetto dei principi ivi contenuti;

- l'adozione e attuazione di procedure;
- l'adozione e la diffusione di "comunicazioni organizzative" che descrivono responsabilità e compiti delle varie funzioni e garantiscono un aggiornamento dinamico dell'organigramma;
- l'adozione di sistemi di protezione da software pericolosi (es. worm e virus);
- il blocco automatico dell'accesso ai siti rientranti nella black list di riferimento;
- l'indicazione di specifiche istruzioni in merito alla gestione degli strumenti informatici aziendali (es. pc portatili);
- l'adozione delle misure organizzative e tecnico-informatiche richieste in adempimento alla normativa sulla privacy di cui al GDPR.

REPORTING VERSO L'ORGANISMO DI VIGILANZA

Attraverso gli appositi canali dedicati:

- chiunque venga a conoscenza di violazioni del Modello Organizzativo o del Codice Etico o di situazioni di pericolo o anomalie dovrà immediatamente segnalarlo all'OdV;
- chiunque venga a conoscenza di violazioni delle procedure interne adottate in materia dovrà immediatamente segnalarlo all'OdV.

In particolare l'OdV dovrà immediatamente essere informato di:

- eventuali violazioni in materia di tutela del diritto d'autore e/o reati informatici;
- eventuali audit effettuati in materia, sia da parte di funzioni interne che da parte di soggetti esterni incaricati.