FONDAZIONE
EDMUND MACH

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ex D. Lgs. n. 231/2001

– Parte Speciale 2 –

Reati Informatici
Reati in violazione del diritto d'autore

Adottato con deliberazione del CdA n. 1 del 26/5/2015, con efficacia dal 1/7/2015.
Primo aggiornamento – riguardante le novità legislative sui reati societari (parte speciale 6) e sui reati ambientali (parte speciale 8) – adottato con deliberazione del CdA n. 11 del 23/6/2015
Secondo aggiornamento – di carattere generale, a seguito della riorganizzazione interna – adottato con deliberazione del CdA n. 23 del 15/06/2017.
Terzo aggiornamento – di carattere generale e particolare, con riferimento alle novità legislative sui reati contro la PA (parte speciale 1) e sui reati tributari (parte speciale 6) nonché introduzione della parte dedicata ad altri reati (parte speciale 10) – adottato con deliberazione del CdA n. 33 del 24/5/2021.

SOMMARIO

1. LE FATTISPECIE DEI REATI INFORMATICI (ART. 24, LIMITATAMENTE ALLA FRODE INFORMATICA, E ART. 24 *BIS* DEL D. LGS. N. 231/2001)

L'art. 24 *bis* è stato introdotto, nel corpo del D. Lgs. n. 231/2001, dalla L. n. 48/2008, di ratifica della c.d. Convenzione Cybercrime, firmata a Budapest il 23 novembre 2001. L'introduzione di tale tipologia di reati nel novero delle fattispecie idonee a generare la responsabilità dell'ente ha un'importanza pratica assai rilevante, constatato che, in questo momento storico, ogni realtà aziendale, di qualsivoglia dimensione, si avvale di sistemi informatici più o meno sofisticati.

Prima di procedere all'illustrazione di singoli "reati presupposto", è opportuno chiarire che cosa si intenda per "**sistema informatico**" e cosa per "**dato informatico**".

L'art. 1 della citata Convenzione stabilisce che per "**sistema informatico**" deve intendersi **qualsiasi dispositivo o qualsiasi gruppo di dispositivi tra loro interconnessi o collegati, uno o più dei quali, in base ad un programma, eseguono l'elaborazione automatica dei dati**. La principale caratteristica di un "sistema informatico" è dunque l'esecuzione automatizzata di operazioni.

Per "**dato informatico**", la stessa Convenzione intende q**ualsiasi rappresentazione di fatti, informazioni o concetti in una forma che ne permetta l'elaborazione con un sistema informatico**. Tale definizione fa riferimento sia ai dati in senso stretto, sia ai programmi, in quanto i primi costituiscono le informazioni che vengono generate e salvate attraverso l'utilizzazione dei secondi.

Le singole fattispecie contemplate nel D. Lgs. n. 231/2001 all'art. 24 *bis* sono le seguenti:

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

L'art. 615 *ter* c.p. sanziona, con la reclusione fino a tre anni, chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Sono inoltre previste pene più severe (reclusione da uno a cinque anni) nel caso in cui:

a) il fatto sia commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

b) se il colpevole, per commettere il fatto, usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

c) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Un ulteriore aumento del carico sanzionatorio è previsto nel caso in cui le condotte sopra descritte abbiano ad oggetto sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

La norma è posta a tutela della c.d. riservatezza informatica o, secondo alcuna giurisprudenza, del c.d. domicilio informatico. Attraverso le misure di sicurezza (che, secondo la giurisprudenza, possono essere sia fisiche che logiche) poste a tutela della singola postazione informatica ovvero della rete informatica o telematica, il titolare del sistema informatico manifesta il c.d. *ius excludendi alios*, ovvero il diritto di negare, a terzi non autorizzati, l'utilizzazione della macchina o la connessione al sistema informatico. Il parallelismo con il domicilio fisico ha riscosso particolare fortuna: come è punito chi si introduce in una privata dimora o nelle sue pertinenze senza il consenso di chi ha il diritto di escluderlo (sia esso il proprietario o l'utilizzatore), così è punito chi si introduce negli altrui sistemi informatici, senza il consenso di chi vanta, su quei medesimi sistemi, un diritto di filtrare gli utenti.

L'art. 615 *ter* c.p. è fattispecie penale applicabile nel caso di azioni di *hackeraggio* o di *crackeraggio*.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.)

La norma sanziona (con la reclusione sino ad un anno e con la multa sino a € 5.164,00) chi riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

In determinati casi, la pena è aumentata.

Si tratta di un delitto evidentemente prodromico rispetto al reato di cui all'art. 615 *ter* c.p. Questa ultima norma – come illustrato sopra – punisce chi ha effettuato un accesso abusivo ad un altrui sistema informatico; mentre l'art. 615 *quater* c.p. appresta una tutela anticipata sanzionando chi, con l'evidente finalità di facilitare o compiere un accesso abusivo a sistema informatico, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi aventi la specifica finalità di consentire l'accesso ad un sistema informatico o telematico protetto da misure di sicurezza.

Ad esempio, sarà punibile ai sensi dell'art. 615 *quater* c.p. chi diffonda o consegni a terzi (in rete o *brevi manu*) il codice PIN che consente di operare con una tessera bancomat; gli *user–name* e le *password* che permettono di movimentare somme di denaro a mezzo *home banking*; le credenziali di accesso ad un sito di acquisti o vendite *on line*.

Danneggiamento di informazioni, dati e programmi informatici (artt. 635 *bis*, *ter quater* e *quinquies* c.p.)

Il c.d. danneggiamento informatico, fino al 2008 era sanzionato da un'unica norma, l'art. 635 *bis* c.p., che prevedeva la reclusione da sei mesi a tre anni per chi chiunque *"distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui"*.

Come accennato, nel 2008 la L. n. 48 ha abrogato l'art. 635 *bis* sostituendolo con altre quattro norme:

a) l'art. 635 *bis* c.p. punisce ora il danneggiamento di informazioni, dati e programmi informatici ad uso privato;
b) l'art. 635 *ter* c.p. punisce il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
c) l'art. 635 *quater* c.p. punisce il danneggiamento di sistemi informatici o telematici ad uso privato;
d) l'art. 635 *quinquies* c.p. punisce il danneggiamento di sistemi informatici o telematici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

Tutte e quattro le norme sono richiamate dall'art. 24 *bis* del D. Lgs. n. 231/2001 e quindi, nel caso in cui uno dei descritti illeciti sia commesso da soggetto appartenente alla FEM (che si trovi in posizione apicale o sottordinata) può aversi una responsabilità della FEM stessa.

Mentre la norma sull'accesso abusivo sanziona semplicemente chi si introduce in un sistema informatico, a prescindere dal fatto che questa condotta rechi o meno un danno al sistema informatico stesso (si pensi, ad esempio, ad un fenomeno di spionaggio industriale, che può essere perpetrato anche senza il danneggiamento del sistema), gli artt. 635 *bis*, *ter, quater* e *quinquies* riguardano, invece, proprio la condotta di chi, indipendentemente dall'abusività dell'accesso, danneggi il sistema, alterandone il funzionamento.

L'esempio più classico è quello dei *virus* informatici, che, solitamente trasmessi con strumenti auto–replicanti, fanno compiere al sistema azioni pregiudizievoli, con ciò danneggiandolo.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.)

L'art. 615 *quinquies* c.p. sanziona chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Anche in questo caso si tratta di una condotta prodromica rispetto al danneggiamento vero e proprio, tant'è che la pena è inferiore.

Come capita in altri settori dell'ordinamento, anche in materia di criminalità informatica il legislatore ha ritenuto che attendere la verificazione dell'effettivo evento lesivo per comminare la sanzione possa, in qualche modo, vanificarne l'utilità. Di qui l'anticipazione della soglia di rilevanza penale: ribadita la sanzione per chi effettivamente danneggia un sistema informatico o telematico, il codice penale non rinuncia a sanzionare anche chi tiene un comportamento che, comunque, è diretto in modo non equivoco al danneggiamento.

Continuando nell'esempio, è prevista una sanzione penale tanto per chi, diffondendo un *virus*, riesce nell'intento di danneggiare un sistema informatico, quanto per chi, a prescindere dal verificarsi del danneggiamento, comunque diffonde un programma (nella specie, un *virus*) con lo specifico intento di danneggiamento.

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

L'art. 617 *quater* ha un duplice contenuto sanzionatorio. È, infatti, prevista una pena per chi:

a) fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe;

b) rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni fraudolentemente intercettate.

La ragione della norma sta nella tutela del diritto alla segretezza ed alla integrità delle comunicazioni.

Dal 1974 il codice sanziona penalmente chi intercetta comunicazioni di natura telefonica o telegrafica (art. 617 c.p.). Analoga sanzione è prevista, dal 1993, per chi tiene la stessa condotta su di un oggetto materiale informatico o telematico.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)

Valgano, anche in questo caso, le considerazioni che si sono fatte per gli artt. 615 *quater* e *quinquies* c.p., visto che la norma sanziona chi installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491 *bis* c.p.)

L'art. 491 *bis* c.p. prevede che se alcuna delle falsità previste dal libro II, titolo VII, capo III del codice penale riguarda un documento informatico, pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del medesimo capo concernenti rispettivamente gli atti pubblici e le scritture private.

Per effetto dell'art. 491 *bis* c.p., quindi, i reati in materia di falso risultano applicabili anche se l'oggetto materiale della condotta è costituito dal documento informatico. L'estensione, prevista fin dal 1993, si è resa necessaria in ragione del fatto che i delitti a tutela della fede pubblica sono stati pensati dal legislatore del 1930 avendo riguardo, essenzialmente, al documento cartaceo.

Le norme su cui ha effetto l'estensione prevista dall'art. 491 *bis* c.p. sono numerose e complesse (dall'art. 476 all'art. 491 c.p.). Tra esse, tuttavia, assumono un'importanza sicuramente prevalente le fattispecie di c.d. falso materiale e di c.d. falso ideologico.

Si configura un reato di falso materiale quando un pubblico ufficiale (art. 476 c.p.) o un privato cittadino (art. 482 c.p.) forma un atto falso ovvero altera un atto vero.

Si configura invece un reato di falso ideologico nel caso in cui un pubblico ufficiale, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità (art. 479 c.p.). Il privato cittadino è punito a titolo di falso ideologico quando attesta a pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità (art. 483 c.p.) ovvero quando, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri danno, abusa di foglio firmato in bianco, scrivendovi un atto produttivo di effetti giuridici diverso da quello a cui era obbligato o autorizzato.

Altre norme hanno minore importanza.

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

Trattasi di fattispecie molto settoriale, che ha ad oggetto l'attività del "certificatore qualificato", ovvero di quel soggetto, pubblico o privato, che è abilitato al rilascio di quella particolare forma di firma elettronica nota con il nome di "firma digitale".

Il certificatore, oltre ad avere una funzione di natura puramente tecnica (di solito è colui che fornisce il servizio PEC attraverso le *smart–card* o strumenti similari), ha anche una caratterizzazione di stampo pubblicistico. Il sistema informatico delle firme digitali è congeniato in maniera tale per cui un *server*, che funge da trasportatore del messaggio elettronico, certifica al destinatario X che il messaggio proviene dal mittente Y. Detto diversamente, il destinatario X sa che il messaggio proviene sicuramente dal mittente Y perché solo il mittente Y possiede la chiave di cifratura specificamente usata nel messaggio inviato. La funzione del certificatore è, appunto, quella di dare la garanzia che Y sia in rete chi effettivamente egli è nella realtà. Allo scopo, al momento del rilascio della chiave crittografica (contenuta nella *smart–card* che serve per crittografare i messaggi di posta elettronica e, quindi, firmarli digitalmente), il certificatore è tenuto ad identificare compiutamente il soggetto richiedente. Il certificatore identifica la persona fisica Y (ad esempio a mezzo dei documenti di identità) ed attesta che la chiave di crittografia viene rilasciata solo ad Y.

La funzione del certificatore è quindi molto importante, perché attesta la corrispondenza tra i soggetti reali e la loro proiezione virtuale.

L'art. 640 *quinquies* c.p. sanziona quel certificatore che, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, con ciò ingenerando un falso affidamento nei consociati.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.)

Il reato di frode informatica è previsto dall'art. 24 del D. Lgs. n. 231/2001, dedicato ai reati contro la Pubblica Amministrazione, anziché nell'art. 24 *bis* del Decreto, dedicato ai reati informativi. *Ratione materiae*, si è però preferito affrontarne l'analisi in questa Parte Speciale.

Tale ipotesi di reato sanziona chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

La pena è aumentata se il fatto è commesso a danno dello Stato o di un altro ente pubblico ovvero se il fatto è commesso con abuso della qualità di operatore del sistema ovvero se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

2. LE FATTISPECIE DEI REATI IN MATERIA DI TUTELA DEL DIRITTO D'AUTORE (ART. 25 *NOVIES* DEL D. LGS. N. 231/2001)

L'art. 25 *novies* richiama la L. n. 633/1941, contenente la disciplina organica del diritto d'autore (c.d. LDA).

Le singole fattispecie contemplate nel D. Lgs. n. 231/2001 all'art. 25 *novies* sono le seguenti:

Art. 171 della L. n. 633/1941

Racchiude le sanzioni penali residuali. In applicazione del principio di specialità, se il fatto concreto può essere sussunto in una delle fattispecie di cui all'artt. 171 *bis* o 171 *ter*, l'art. 171 non può trovare applicazione.

Art. 171, comma 1, lettera a–bis) e comma 3 della L. n. 633/1941

L'art. 171, comma 1, lett. a–*bis*) LDA., introdotto nel 2005, sanziona chi 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.

Si tratta, in sostanza, del diffuso fenomeno della condivisione in rete di materiale protetto dalla normativa sul diritto d'autore.

Il comma 3 del medesimo art. 171, pure richiamato dal D. Lgs. n. 231/2001, si occupa di ipotesi più specifiche di violazione del diritto d'autore.

Art. 171 *bis* della L. n. 633/1941

L'art. 171 *bis* tutela i programmi informatici. Esso sanziona una vasta serie di comportamenti. In particolare, è prevista una sanzione penale per chi 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 altresì sanzionato chi duplica, importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione 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.

Altri fatti aventi rilevanza penale sono previsti al comma 2 del medesimo articolo, in relazione a: trasferimento, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, estrazione o reimpiego, vendita o concessione in locazione di banche dati.

Art. 171 *ter* della L. n. 633/1941

La norma si occupa di tutelare le opere dell'ingegno destinate 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.

È sanzionata praticamente ogni condotta di illecita duplicazione o diffusione.

Art. 171 *septies* della L. n. 633/1941

Prevede una sanzione per i produttori o gli importatori dei supporti non soggetti al contrassegno di cui all'art. 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.

È altresì sanzionato chi dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'art. 181 *bis*, comma 2 LDA in materia di SIAE.

Art. 171 octies della L. n. 633/1941

La norma sanziona 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.

3. PROCESSI SENSIBILI NELL'AMBITO DEI REATI INFORMATICI E DEI REATI POSTI A TUTELA DEL DIRITTO D'AUTORE

Costituiscono un rischio rispetto alla commissione dei reati sopra elencati le seguenti attività:

a) scorretto uso di personal computer, *tablet*, *smartphone* o altri dispositivi che permettono il collegamento a internet affidati all'utente;
b) scorretto uso di dispositivi *hardware* o *software* della FEM o personali;
c) scorretto uso della rete della FEM;
d) scorretto uso della posta elettronica;
e) scorretto uso della rete *internet* e dei relativi servizi;
f) uso scorretto delle postazioni autogestite collegate alla rete della FEM;
g) uso scorretto credenziali di accesso alla rete;
h) indebita duplicazione o copiatura di opere intellettuali protette dal diritto d'autore;
i) usurpazione di un titolo di proprietà industriale.

4. LOGICHE COMPORTAMENTALI DI ORDINE GENERALE

È fatto espresso divieto agli organi statutari della FEM, ai dipendenti ed ai consulenti di:

a) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 – con riferimento all'art. 640 *ter* c.p.; 24 *bis* e 25 *novies* del D. Lgs. n. 231/2001);
b) violare i principi e le procedure interne contenute nel Regolamento ICT della Fondazione Edmund Mach (allegato B.23 del ROF) e della relativa procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM
c) compiere qualunque tipo di operazione che rechi rischio per la sicurezza della rete informatica della FEM.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo, a carico dei soggetti sopra indicati, di:

a) tenere un comportamento corretto, nel rispetto delle norme di Legge e delle procedure interne, in tutte le attività che importino l'uso dei sistemi informatici (compresi gli strumenti di posta elettronica e l'accesso ad *internet*);
b) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità dei sistemi informatici, a tutela dei dati personali e a tutela del diritto d'autore;
c) assicurare il regolare funzionamento dei sistemi informatici, attenendosi alle procedure impartite ed agevolando ogni forma di controllo interno;
d) dare seguito con tempestività alle prescrizioni impartite in materia di uso dei sistemi informatici.

5. PROCEDURE SPECIFICHE

Come specificato nel Regolamento ICT della Fondazione Edmund Mach (ROF – all. B.23) e della relativa procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM, è fatto obbligo ai Destinatari di:

a) rispettare le norme disciplinanti le attività e i servizi che si svolgono nella rete;

b) non commettere abusi e non violare i diritti degli altri utenti e dei terzi;
c) assumere la totale responsabilità delle attività svolte tramite la rete stessa;
d) mantenere in efficienza e in buono stato la posizione assegnata o concessa in uso, attuando tutto il possibile per proteggere macchinari e software da danneggiamenti accidentali o colposi;
e) conservare ed utilizzare le credenziali fornite (utente–*password*) per uso esclusivamente personale. Il titolare è responsabile delle attività svolte tramite le stesse.

È fatto divieto di utilizzare la rete:

a) in modo difforme da quanto previsto nel Regolamento ICT della Fondazione Edmund Mach (allegato B.23 del ROF) e della relativa procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM;
b) (per i soli utenti CRI) in modo difforme dalle regolamentazioni dettate dai responsabili della rete nazionale della ricerca GARR;
c) in modo difforme da quanto previsto dalle leggi penali, civili e amministrative in materia di disciplina delle attività e dei servizi svolti sulla rete;
d) per scopi incompatibili con le finalità e con l'attività istituzionale della FEM così come stabilito nel suo Statuto;
e) per conseguire l'accesso non autorizzato a risorse di rete internet od esterne della FEM;
f) per commettere attività che violino la riservatezza di altri utenti o di terzi;
g) per attività che influenzino negativamente la regolare operatività della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti;
h) per attività che distraggano risorse (persone, capacità, elaboratori);
i) per attività che provochino trasferimenti non autorizzati di informazioni (*software*, basi dati, etc.) proprietarie;
j) per attività che violino le leggi a tutela delle opere dell'ingegno.

È inoltre vietato usare l'anonimato o servirsi di risorse che consentono di restare anonimi.

Nell'espletamento di tutte le operazioni attinenti le attività della FEM, gli organi statutari della FEM, i dipendenti ed i consulenti (nella misura necessaria alle funzioni dagli stessi svolte) devono conoscere e rispettare:

a) il **Regolamento proprietà intellettuale e imprese *spin–off*** (ROF – all. B19);
b) il **Regolamento dei servizi della Biblioteca della Fondazione Edmund Mach** (ROF – all. B5);
c) il **Regolamento per la gestione della proprietà intellettuale generata dalla Fondazione Edmund Mach** (ROF – all. B10);
d) il **Regolamento afferente ai centri operativi (CRI e CTT) in merito alla protezione e valorizzazione della proprietà intellettuale generata in Fondazione Edmund Mach** (ROF – all. B12);
e) il **Regolamento sui diritti di proprietà intellettuale relativi ai risultati della ricerca della Fondazione Edmund Mach** (ROF – all. B24);
f) il **Regolamento ICT della Fondazione Edmund Mach** (ROF – all. B23);

Procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM

g) la **Procedura per l'inventario dei beni.** Importante, ai fini della presente parte speciale: a. nella sua disciplina circa l'inventario di beni mobili, inclusi *computer* ed apparecchiature informatiche, *software* di proprietà, brevetti; b. nella parte in cui disciplina l'inventario del materiale bibliografico (specificando che i volumi sono inventariati al prezzo di copertina, anche se pervenuti a mezzo di liberalità, oppure al valore di stima, se non è indicato alcun prezzo);
h) in generale, la normativa applicabile alla materia, tra cui: L. n. 547/1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*; L. n. 48/2008 *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*; D. Lgs. n. 196/2003, *Codice in materia di protezione dei dati personali*; L. n. 633/1941, *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*; la LP. 14/2005, *Legge Provinciale sulla ricerca*, nella parte in cui disciplina brevetti e diritti di proprietà intellettuale delle Fondazioni.

Oltre ai documenti sopra richiamati, i Destinatari afferenti al Centro di Ricerca e innovazione sono tenuti a conoscere e rispettare:

a) le regole comportamentali contenute nel documento denominato *"**Acceptable Use Policy della rete GARR – Rete Italiana dell'Università e della Ricerca**"*;
b) i *"**Quaderni di Laboratorio**"*, strumento obbligatorio per tutto il personale attivo in laboratorio del Centro Ricerca e Innovazione (Dipendenti CRI (TD e TI), contrattisti, borsisti, tirocinanti e frequentatori che svolgono attività di ricerca o vi partecipano a qualunque titolo), il cui scopo è contribuire alla difesa della proprietà intellettuale e permettere una migliore gestione e monitoraggio dei progetti;
c) il "***Manuale breve della Fondazione Edmund Mach in tema di proprietà intellettuale e trasferimento***

della conoscenza".

La FEM ha adottato la procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM tenendo conto delle novità introdotte nello statuto dei lavoratori e di quelle previste dal Regolamento UE 2016/679 in materia di protezione dei dati personali. Con tale aggiornamento la FEM ha formalizzato all'interno di tale procedura la disciplina della nomina e controllo degli Amministratori di Sistema (interni ed esterni) ed ha provveduto alla nomina di un Responsabile della Protezione dei Dati personali (RPD/DPO).

6. I CONTROLLI DELL'ODV

L'OdV effettua periodicamente:

a) interrogazioni agli amministratore di sistema sull'assetto del sistema informatico e sui controlli effettuati;
b) controlli a campione sull'uso dei sistemi informatici da parte degli utenti;
c) verifica delle attività di formazione svolte;
d) controlli sulla corretta procedura di *backup*;
e) in generale, ogni controllo diretto a verificare la sicurezza dei sistemi informatici e della rete informatica;
f) in generale, ogni controllo diretto a verificare il rispetto della normativa in materia di tutela del diritto d'autore.

Resta fermo il potere discrezionale dell'OdV di attivarsi con specifici controlli anche a seguito di segnalazioni ricevute.

All'OdV viene garantito libero accesso a tutta la documentazione della FEM e ad ogni registro informatico.

7. FLUSSI INFORMATIVI VERSO L'ODV

L'OdV deve essere informato:

Oggetto flusso informativo	Struttura responsabile	Destinatari	Tempistica
Disfunzioni o lacune del sistema informatico segnalate dagli utenti agli amministratori di sistema.	**DG** Ripartizione Sistemi Informativi e Comunicazione	OdV	Annuale
Acquisto di *hardware* e *software* di particolare rilievo per la FEM, principali attività svolte, eventuali criticità riscontrate.	**DG** Ripartizione Sistemi Informativi e Comunicazione	OdV	Annuale
In materia di trattamento dei dati personali, relazione circa l'attività di controllo eseguita sugli Amministratori di Sistema.	**DG** (Ripartizioni) **CENTRI** (CIF – CRI – CTT)	OdV	Tempestiva