



## **Regolamento per un Uso Accettabile e Responsabile di Internet (P.U.A.)**

***Approvato Con Delibera n. 25 del Consiglio d'istituto del 23 dicembre 2020***

### ***Introduzione e indicazioni sul processo di revisione***

*Le PUA sono parte integrante del DPS e sono pubblicate sul sito della scuola. La revisione è periodica, ad opera del Dirigente Scolastico.*

### ***Contenuti***

1. I vantaggi di internet a scuola
2. Accertamento dei rischi e valutazione dei contenuti di internet
  - 2.1. Materiale non consono allo stile educativo della scuola
  - 2.2. Azioni illecite
  - 2.3. Privacy
  - 2.4. Diritti d'autore
3. Le strategie della scuola per garantire la sicurezza delle TIC
4. Norme e linee guida
  - 4.1. Utilizzo dei servizi Internet
  - 4.2. Posta elettronica
  - 4.3. Altre forme tecnologiche di comunicazione
  - 4.4. Mailing list moderate, gruppi di discussione blog e chat room
5. La gestione del sito della scuola
6. Servizi on line alle famiglie/utenti esterni
  - 6.1. Registro on-line (Axios)
7. Altre forme tecnologiche di comunicazione
8. Informare sulla PUA della scuola
  - 8.1. Informare gli studenti sulla PUA della scuola
  - 8.2. Informare il personale scolastico della PUA
  - 8.3. Informare i genitori/tutori sulla PUA della scuola
9. Netiquette
10. Operazioni non Autorizzate
11. Reati e violazioni della legge

## 1 - I vantaggi di internet a scuola

La Rete Internet offre, sia agli studenti che agli insegnanti, una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi; permette di trovare materiale, recuperare documenti e scambiare informazioni. Inoltre, su Internet, si possono recuperare risorse per le attività scolastiche e sociali.

La nostra scuola organizza molte attività che possono trarre giovamento dall'uso della rete. I programmi di quasi tutte le nostre materie prevedono ricerche di materiale di vario tipo, utilizzo di documenti e scambio d'informazioni.

Alcuni progetti del POF prevedono aperture pomeridiane delle aule di Informatica e dei laboratori con presenza di almeno un docente esperto per attività al computer: *studio, ricerche, IDEI, preparazione alla ECDL, certificazioni, CLIL, ecc..*

Sulla rete, poi, si possono trovare informazioni e risorse per il tempo libero, le attività scolastiche e sociali.

La rete interna della scuola è un ottimo strumento di comunicazione sia sul piano amministrativo burocratico sia su quello didattico ed un indispensabile strumento di manutenzione e controllo.

La rete Internet e il sito dell'Istituto sono destinate a diventare formidabili ed economici mezzi di comunicazione tra famiglie, docenti, personale e della scuola e studenti.

La nostra scuola, *per convinzione e nel rispetto della normativa vigente*, intende favorire **l'utilizzo responsabile di Internet** per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse.

## 2 - Accertamento dei rischi e valutazione dei contenuti di internet

Da una parte le leggi dello stato impongono alle scuole l'uso di internet e i finanziamenti lo rendono possibile, dall'altra, i pericoli insiti nella rete (*molestie e contatti con materiali non consoni*) e altre norme dello stato e comunitarie, (*come quelle sulla privacy e sui diritti d'autore*) ne ostacolano l'uso in modo notevole e possono scoraggiare o spaventare chi vorrebbe sperimentare le nuove possibilità offerte dall'uso delle tecnologie e chi ha responsabilità.

La scuola si rende conto che non è possibile evitare *in modo totale* che gli studenti - trovino materiale indesiderato navigando su un computer della scuola - o possano compiere, *perfino inconsapevolmente*, azioni illecite.

La nostra esperienza ci ha tuttavia insegnato che, promuovendo un **uso consapevole e sicuro** della rete e adottando i provvedimenti previsti in questo documento il controllo dei rischi diventa possibile e i rari incidenti, affrontati con la dovuta serenità, possono perfino diventare opportunità formative.

### 2.1. Materiale non consono allo stile educativo della scuola

Gli alunni devono essere guidati a riconoscere i rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere ed a evitare gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli studenti non deve essere sottoposto materiale di questo tipo e se ne vengono in contatto devono sempre riferirlo all'insegnante o al responsabile di laboratorio per le segnalazioni del caso alle autorità competenti.

### 2.2. Azioni illecite

Nonostante i filtri e la sorveglianza, coi computer di una scuola si possono compiere azioni illecite di vario tipo: (Calunnie, molestie, perfino furti...). A volte l'illecito può avvenire senza la consapevolezza di chi lo provoca (è il caso di chi clicca senza leggere...).

La scuola prende due tipi di precauzioni: adozione di filtri e strumenti tecnici atti ad impedire questo tipo di cose e di norme di comportamento conosciute e condivise.

### 2.3. Privacy

Per quanto riguarda la privacy l'informatizzazione della gestione dei dati aumenta le garanzie a patto che si prendano le dovute precauzioni.

I principali rischi che si riferiscono all'utilizzo di computer per la gestione degli archivi presi in considerazione in questo documento sono i seguenti:

-Rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati.

-Rischio interno dovuto a intrusioni da parte di studenti.

-Rischio esterno relativo all'accesso ai dati da parte di persone estranee attraverso eventuali punti di ingresso/uscita verso internet.

-Rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker.

-Rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.

L'invio e la ricezione di messaggi E-mail da e verso la scuola è soggetto a regole e precauzioni particolari.

## **2.4. Diritti d'autore**

La scuola rispetta la normativa sui diritti d'autore sia proibendo a docenti, allievi e personale l'installazione di software senza preventiva autorizzazione e controllo, sia insegnando agli alunni ad evitare il plagio nell'utilizzo di materiali provenienti da Internet.

## **3 - Strategie della scuola per garantire la sicurezza delle TIC**

**- Separazione della rete didattica dalla rete amministrativa.**

**- Il materiale presente sullo spazio web della scuola è periodicamente controllato dal D.S. e dal referente del sito web.**

**- La prevenzione del plagio e delle copie illegali** terrà conto della Legge del 22 aprile 1941 n° 633 art. 70, che recita:

*"il riassunto, la citazione o la riproduzione di brani o di parti di opera per scopi di critica di discussione ed anche di insegnamento, sono liberi nei limiti giustificati da tali finalità e purché non costituiscano concorrenza all'utilizzazione economica dell'opera".*

Sarà quindi permesso l'inserimento a scopo di discussione, di critica, di informazione culturale, parti di opere, brevi estratti o citazioni (mai l'opera integrale) menzionando chiaramente il nome dell'autore e la fonte.

## **4 - Norme e linee guida**

Questa sezione contiene le precauzioni le indicazioni operative e le modalità per risolvere le crisi, i compiti e le persone a cui rivolgersi. Non mancano alcune specificazioni sulle scelte dell'Istituto.

### **4.1 Utilizzo dei servizi Internet**

- Anche per proteggere la privacy dei nostri allievi, poi, la rete è progettata in modo che i computer amministrativi non siano accessibili dai computer destinati alla didattica.
- La responsabilità del corretto utilizzo dei computer situati nei laboratori, in biblioteca o altri locali è in primo luogo dei docenti e del personale che gestiscono tali servizi.
- La responsabilità del corretto utilizzo dei computer a disposizione dei docenti, situati nelle aule professori è del docente che li utilizza. Non si debbono utilizzare i computer delle aule didattiche se sono disponibili queste postazioni.
- -Tutti gli utenti connessi ad internet devono rispettare, oltre alle regole presentate in questo documento, la legislazione vigente applicata anche alla comunicazione su internet e la *netiquette* (etica e norme di buon uso dei servizi di rete).
- L'istituto dispone di LIM connesse ad INTERNET e da Laboratori anch'essi connessi: i rischi sono decisamente alti e quindi maggiori saranno le precauzioni da adottare.
- L'insegnante che accompagna gli allievi in aula computer o utilizza la LIM, è responsabile di quanto avviene. Detta responsabilità è costituita, oltre che dall'obbligo di sorvegliare attivamente le attività, nel dovere di segnalare qualsiasi disagio al personale tecnico o, in loro assenza, di lasciare appositi cartelli sulla macchina su cui si è manifestato il problema. - In alcuni casi, all'atto dell'accesso in internet apparirà una videata che non potrà essere chiusa

senza accettare le norme che vi sono previste. Si ritiene che anche questo sia un modo di responsabilizzare gli utenti. Alcuni siti a rischio sono disabilitati dal firewall.

**Procedura da seguire in caso di segnalazione di molestie, reati o contatto accidentale e non voluto con siti a contenuto decisamente illecito:**

- avvertire subito il tecnico o il responsabile della rete o la vicepresidenza;
- continuare tranquillamente il lavoro (se la cosa è ancora possibile), utilizzando le altre macchine.

Nel cambio d'ora, usciti tutti gli studenti dall'aula, chi di dovere prenderà i provvedimenti del caso. A fronte di violazioni delle regole, la scuola, su valutazione di docenti responsabili della rete e di laboratorio e del dirigente scolastico, si assume il diritto di impedire l'accesso dell'utente a internet per un certo periodo di tempo, rapportato alla gravità.

#### **4.2. Posta elettronica**

- Sui computer dell'istituto si possono utilizzare solo fornitori di servizi e-mail approvati dalla scuola.
- L'invio e la ricezione di allegati sono soggetti al permesso dell'insegnante di classe.
- I docenti che desiderano un account di posta ufficiale per sé devono fare richiesta all'animatore digitale. I docenti sono direttamente responsabili del contenuto della posta inviata o trasmessa al loro account.

#### **4.3 Altre forme tecnologiche di comunicazione**

Agli alunni non è permesso utilizzare i telefoni cellulari durante le lezioni o durante l'orario scolastico. È vietato inviare messaggi illeciti o inappropriati.

#### **4.4 Mailing list moderate, gruppi di discussione blog e chat room**

La scuola utilizza liste di indirizzi di utenti selezionati per distribuire del materiale. E' stato attivato l'ambiente Google for education che utilizza l'account Tale ambiente consente la formazione di gruppi di discussioni, di chat e di classi virtuali.

Gli insegnanti saranno i moderatori degli altri mezzi di collaborazione, dei gruppi di discussione e delle chat room se sono utilizzati a fini scolastici.

- Agli studenti non è consentito l'accesso alle chat room pubbliche o non moderate. - Sono permesse solo chat a scopi didattici e comunque sempre con la supervisione dell'insegnante.
- Gli studenti possono iscriversi a gruppi di discussione che hanno obiettivi e contenuti didattici o collegati alle attività promosse dalla scuola.

### **5 - Gestione del sito web della scuola**

La gestione del sito e dei servizi di rete della nostra scuola è affidata a -----ed personale interno dotato di competenze e in grado di gestire e progettare reti interne e siti web. L'istituto partecipa alle attività di aggiornamento ed è in contatto con le reti territoriali relativi a tale campo.

Il sito è stato concepito nell'osservanza delle linee guida ministeriali e con utilizzo di tecnologie semplici ed intuitive ma sicure, per allargare il più possibile la cerchia dei collaboratori diretti e indiretti. Lo spazio viene fornito su server sicuri ed accessibili solo da postazioni debitamente certificate.

Il Dirigente Scolastico autorizza di volta in volta la gestione delle pagine del sito.

Tutto il personale della scuola è tenuto a segnalare al referente eventuali errori o disfunzioni del sito della scuola di cui sia a conoscenza. Genitori, alunni e utenti del sito sono incoraggiati a fare altrettanto.

**Contenuti:** salvo precisazioni ben visibili sul documento la scuola detiene i diritti d'autore di ciò che si trova sul sito.

**Collegamenti** Anche se l'istituto non può essere considerato responsabile dei contenuti dei siti esterni con cui è collegato, il controllo sui link è tenuto nella massima considerazione, webmaster e referenti per la privacy e la comunicazione effettuano controlli periodici e tutto il personale è tenuto a segnalare qualsiasi problema. Genitori, alunni e utenti del sito sono incoraggiati a fare altrettanto.

**Le informazioni relative alle persone** pubblicate sul sito della scuola devono includere solo l'indirizzo della scuola e indirizzi di posta elettronica ufficiali e il telefono della scuola, ma non

informazioni relative agli indirizzi del personale della scuola o alle loro e-mail private, salvo precisa autorizzazione da parte dell'interessato.

**Il materiale prodotto dagli alunni** minorenni e le loro fotografie saranno pubblicati solo a fini documentativi; si farà sempre in modo che il nome non possa essere collegato ai ritratti. Le fotografie sono selezionate attentamente dagli insegnanti redattori in modo tale che gruppi di alunni siano ritratti in attività didattiche.

## **6 - Servizi on line alle famiglie/utenti esterni**

La scuola offre (all'interno del proprio sito web) tutta una serie di servizi alle famiglie ed agli utenti esterni in continua espansione in base alle richieste dei docenti.

### **6.1 - Registro on-line e comunicazioni scuola-famiglia**

I genitori/tutori, gli alunni maggiorenni ed i docenti possono accedere al registro on-line solo previo inserimento del codice di accesso che è strettamente personale.

Di qui l'invito ai docenti ed ai coordinatori di classe di usare più estesamente tale mezzo di comunicazione ed alle famiglie di verificare periodicamente il registro on-line.

**Si precisa che i servizi offerti non trattano dati sensibili**, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

## **7 - Altre forme tecnologiche di comunicazione**

Agli studenti non è permesso utilizzare gli smartphone o tablet durante le lezioni o durante l'orario scolastico, salvo un uso didattico concordato con i docenti.

È vietato inviare messaggi illeciti o inappropriati,

La normativa in materia di esami di stato è molto severa riguardo al possesso ed uso di cellulari durante lo svolgimento delle prove.

La scuola si uniforma alla direttiva n. 104/2007 del Ministro della Pubblica Istruzione avente per obiettivo quello di contrastare abusi e prassi di utilizzo non corretto di telefoni cellulari e apparecchi analoghi, che consentono la registrazione di files audio e video. È bene precisare che la Direttiva riguarda i comportamenti dei soggetti che interagiscono dentro la comunità scolastica come "privati", in un'ottica di prevenzione e repressione. Resta fuori dalla sua applicazione tutto ciò che è "riconducibile allo svolgimento di attività didattiche, formative o di apprendimento". L'inosservanza della normativa vigente comporta sanzioni penali (artt. 615bis, 528, 594, 600-ter, L.269/98 del CP), civilistiche (artt. 10 CC e art 96 L633/1941), amministrative (art.161 Codice Privacy), e disciplinari (Regolamento d'Istituto)

## **8 - Informare sulla Politica d'Uso Accettabile (PUA) della scuola**

### **8.1 Informare gli studenti sulla PUA della scuola**

Le regole di base relative all'accesso ad internet verranno esposte vicino ad ogni laboratorio di informatica e sulle pagine iniziali di internet.

Gli studenti saranno informati che l'utilizzo di internet è monitorato ed avranno istruzioni per un uso responsabile e sicuro di internet.

### **8.2. Informare il personale scolastico della PUA**

Il personale scolastico avrà una copia all'Albo della Politica d'Uso Accettabile (PUA) della scuola ed è consapevole che l'uso di internet verrà monitorato e segnalato e tutto il personale scolastico sarà coinvolto nello sviluppo delle linee guida della Politica d'Uso Accettabile della scuola e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di internet come richiesto.

**Gli insegnanti firmeranno il documento che riporta le regole per un Uso Accettabile e Responsabile di internet.**

In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il dirigente scolastico o il responsabile della rete per evitare malintesi. Gli insegnanti sono tenuti al corrente delle tematiche concernenti le problematiche sui diritti d'autore che vengono applicate alla scuola.

**8.3 Informare i genitori/tutori sulla PUA della scuola**

I genitori/tutori vengono informati della PUA tramite il sito web della scuola.

**9 - Netiquette**

Fra gli utenti dei servizi telematici di rete si è sviluppata, nel corso del tempo, una serie di tradizioni e di norme di buon senso che costituiscono la "Netiquette" che si potrebbe tradurre in "Galateo (Etiquette) della Rete (Net)": il Galateo della rete.

L'uso di Internet e dei social network ci ha reso cittadini digitali, ma la cittadinanza digitale non è garantita dalla tecnica e dalla destrezza nell'uso delle nuove tecnologie, bensì da una buona conoscenza del regolamento inerente la navigazione tra i servizi dei social network e le relative applicazioni web ( tipo Youtube, Facebook, ...) nonché dei diritti e dei doveri dell'utente.

Ecco allora le regole da rispettare:

- 1– occorre contribuire a rendere il web un luogo sicuro, pertanto ogni volta che un utente commette un abuso o un errore pubblicando materiale illecito, non idoneo o offensivo, occorre contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza;
- 2– ogni abuso subito o rilevato nella navigazione deve essere segnalato tramite gli strumenti offerti dal servizio per ottenere la rimozione del contenuto. Prima di trasformare un incidente o una bravata in una denuncia alle Autorità competenti vale la pena di segnalare il fatto ai gestori del relativo sito per non incorrere in conseguenze penali e giudiziarie;
- 3– se si condividono informazioni personali, prima della pubblicazione occorre scegliere con cura cosa rendere pubblico e cosa mantenere privato, scegliere con attenzione le amicizie con cui accrescere la propria rete e proteggere la propria identità digitale con password;
- 4– se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non si devono pubblicare video girati di nascosto e dove sono presenti persone filmate senza il loro consenso;
- 5– bisogna evitare di scambiare file con utenti di cui non ci si può fidare, in ogni caso anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine del file ed effettuare un controllo con un antivirus aggiornato;
- 6– se durante una conversazione online l'interlocutore diviene volgare, offensivo o minaccioso si deve abbandonare la conversazione;
- 7– nell'uso di sistemi di file-sharing P2P (Peer-to-peer), evitare di scaricare dei file che possono essere considerati illegali e/o protetti dal diritto d'autore, non aprire mai dei file sospetti (la maggior parte dei programmi P2P contiene spyware e malware). Per motivi di sicurezza la scuola vieta l'utilizzo di questi sistemi;

8- i sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi, quando si invia un messaggio a più destinatari che non si conoscono tra loro, è necessario evitare che i destinatari possano vedere e conoscere i propri indirizzi di posta elettronica;

9 - quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso e di non utilizzare files coperti da copyright;

10 – i contenuti pubblicati sulle applicazioni web dei Social Network hanno diversi livelli di visibilità (es. singoli utenti o tutti gli utenti delle rete) che devono essere tenuti a mente dando a ciascun contributo i corretti livelli di privacy;

11 – quando si contribuisce a pubblicare materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto, evitando di pubblicare materiale inadeguato: ci sono luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori.

12 – la reputazione digitale si diffonde velocemente, pertanto non si devono diffamare altre persone, soprattutto se le stesse non sono presenti sul Social network e non possono accorgersi del danno subito;

13 – è possibile la pubblicazione di foto di alunni purchè queste riguardino momenti positivi di vita scolastica, dal momento che con l'informativa sulla privacy, fornita al momento dell'iscrizione, le famiglie sono state informate dell'evenienza.

## **10 - Operazioni non autorizzate**

a) E' vietato a studenti, docenti e al personale tecnico e amministrativo installare programmi non autorizzati sulle postazioni informatiche della scuola. Qualora fosse necessario, solo ed esclusivamente per fini didattici o amministrativi, installare software non ancora in dotazione alla scuola, la persona direttamente interessata deve produrre apposita richiesta al Dirigente scolastico specificando: tipo di programma, utilizzo, eventuale costo, attività interessate e previste con il programma richiesto.

Solo dopo un'accettazione da parte di una commissione costituita dal Dirigente Scolastico, D.S.G.A., assistenti tecnici e Animatore Digitale, si potrà procedere all'acquisto e all'installazione del software.

b) E' vietata la pubblicazione nel sito della scuola di qualsiasi documento, sia esso didattico o amministrativo, prima che la stessa sia stata autorizzata dal Dirigente Scolastico, che avrà provveduto a vistare il materiale.

c) E' vietata l'installazione di propri programmi; è vietata l'installazione di propri dispositivi senza l'autorizzazione del Dirigente scolastico o senza la preventiva scansione con un valido programma antivirus della scuola.

d) E' vietato modificare i programmi installati nei pc o alterarne le configurazioni agendo su software o hardware.

e) E' vietato accedere ai servizi utilizzando l'account di un altro utente.

## **11.Reati e violazioni della legge**

Alcuni comportamenti, al di là delle regole di normale comunicazione talvolta sono solo apparentemente innocui e possono portare a commettere veri e propri reati con conseguenti procedimenti penali. Si esplicitano alcuni esempi:

## **REATI INFORMATICI**

La legge 547/193 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare di imprese e di enti pubblici:

### ***Accesso abusivo ad un sistema informatico e telematico***

Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC a insaputa del legittimo proprietario, oppure forzare la password di un altro utente e più in generale accedere abusivamente alla posta elettronica, ad un server o ad un sito su cui non siamo autorizzati - 615 ter cp.

### ***Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico***

L'art 615 quinquies punisce "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento". - Per commettere questo reato basta, anche solo per scherzo, diffondere un virus attraverso il messenger o la posta elettronica, spiegare ad altre persone come si può fare per sproteggere un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.

### ***Danneggiamento informatico***

Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui. Art. 635 cp.

### ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici***

Questo particolare reato viene disciplinato dall'art.615 quater cp e si presenta spesso come complementare rispetto al delitto di frode informatica. -E' considerato reato anche quando l'informazione viene fraudolentemente carpirsi con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati o osservando e memorizzando la "digitazione" di tali codici. - Si commette questo reato quando si carpiscono, anche involontariamente, i codici di accesso alla posta elettronica, al messenger o al profilo di amici e compagni.

### ***Frode informatica***

Questo reato discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui 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". Art. 640 ter cp. Il profitto può anche non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale".

- Il delitto di frode informatica molto sovente viene a manifestarsi unitamente ad altri delitti informatici, quali l'accesso informatico abusivo e danneggiamento informatico in conseguenza a detenzione e diffusione abusiva di codici di accesso a sistemi informatici o diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

## **REATI NON INFORMATICI**

Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:

### ***Ingiuria***

Chiunque offende l'onore o il decoro di una persona presente commette il reato di ingiuria. Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.

### ***Diffamazione***

Si verifica quando offende la reputazione di qualcun altro, quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona. Art. 595 cp. Ne è un'aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito Web o social network di una informazione o un giudizio su un soggetto. La pubblicazione on-line, dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando una incontrollabile e inarrestabile diffusione della notizia.

### ***Minacce e molestie***

Il reato di minaccia consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica. Art. 612 cp. Può capitare che alcune minacce vengano diffuse per via telematica anche per finalità illecite ben più gravi: come ad esempio obbligare qualcuno a "fare, tollerare o omettere qualche cosa" (Violenza privata: art. 610 cp.) o per ottenere un ingiusto profitto (Estorsione : art. 629 cp.). Sull'onda di questa tipologia di reati è utile descrivere anche quello di molestie e disturbo alle persone, disciplinato dall'art. 660 cp. che si fonda sul contattare, da parte di terzi, per finalità pretestuose, il soggetto i cui dati sono stati "diffusi" per via telematica. Ad esempio la pubblicazione del nominativo e del cellulare di una persona on-line, accompagnato da informazioni non veritiere o ingiuriose: ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite

### ***Violazione dei diritti d'autore***

La legge n. 633 del 22 aprile 1941 e successive modificazioni, sottolinea all'art. 1, che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali ovvero pone in commercio, detiene per la vendita o introduce a fini di lucro le copie, viola i diritti d'autore. Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti. In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato basta pubblicare su YouTube un video con una qualsiasi musica di sottofondo senza le dovute autorizzazioni. Un'ulteriore possibile violazione del diritto d'autore si verifica quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo, come ad esempio, rivenderlo a terzi o

distribuirlo sulla Rete facendone più copie non autorizzate. La legge italiana sul diritto d'autore consente all'utilizzatore di un software o di un'opera multimediale o musicale di effettuare un'unica copia di sicurezza ad uso personale, utile nei casi di malfunzionamento del programma, smarrimento della copia originale etc. Tale copia, salvo autorizzazione della casa di produzione, non può essere ceduta ad altre persone. La duplicazione abusiva (senza autorizzazione) è sanzionata penalmente e colpisce ugualmente anche chi duplica abusivamente non a scopo di lucro, bensì per un semplice fine di risparmio personale