IIS LAGRANGIA - Vercelli

PUA - POLITICA PER L'USO ACCETTABILE DELLA RETE DI ISTITUTO

Approvata dal Consiglio d'Istituto nella seduta del 16-06-2017

PREMESSA

La presente **Politica per l'Uso Accettabile della Rete di Istituto (PUA)** fornisce le linee guida e le norme di comportamento cui si debbono attenere tutti gli utenti che utilizzino la rete informatico-telematica dell'IIS Lagrangia, siano essi figure del personale interno (docenti, allievi e personale ATA) o siano essi esterni (genitori, personale di altre scuole, di altre amministrazioni o ditte esterne).

Tale **PUA** è esposta nelle aule, nei laboratori e in generale nei locali dell'Istituto che siano luoghi di studio o di lavoro. Inoltre tale **PUA** viene consegnata e sottoscritta preventivamente da tutti coloro che, a vario titolo, richiedano l'accesso alla rete informatico-telematica dell'IIS Lagrangia.

Quindi tutto il personale interno (docenti, allievi e personale ATA) analizzerà la **Politica per l'Uso Accettabile della Rete di Istituto** sottoscrivendola all'inizio dell'anno scolastico o all'inizio del rapporto di lavoro, mentre il personale esterno (genitori, personale di altre scuole, di altre amministrazioni o ditte esterne) analizzerà la **Politica per l'Uso Accettabile della Rete di Istituto** sottoscrivendola prima dell'accesso alla rete stessa.

Per quanto attiene agli allievi, sarà cura del docente coordinatore di classe illustrare loro, anche didatticamente, i contenuti della **Politica per l'Uso Accettabile della Rete di Istituto**, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica in rete.

In particolare i genitori/tutori saranno informati sulla **Politica per l'Uso Accettabile della Rete di Istituto** per un utilizzo responsabile di Internet a scuola e a casa tramite:

- sottoscrizione della stessa per i figli minorenni
- esposizione del presente documento all'Albo di Istituto
- pubblicazione dello stesso sul sito web di istituto: http://www.istitutosuperiorelagrangiavc.it

I genitori/tutori possono inoltre, per qualsiasi dubbio, chiedere consiglio e consulenza ai docenti dell'IIS Lagrangia.

CONTENUTI

ARTICOLO 1. Comportamenti in rete e uso consapevole delle tecnologie dell'informazione e della comunicazione nel rispetto della legge e del galateo

Fra gli utenti dei servizi telematici e di Internet si sono sviluppati nel corso del tempo una serie di principi di buon comportamento che vengono identificati con il nome di Netiquette. In particolare con l'avvento del web2.0 e dei Social Network, basati sui principi di intervento, collaborazione e condivisione diretta da parte degli utenti, Internet e i suoi servizi si sono evoluti dando conseguentemente vita ad un galateo del web2.0 che prende il nome di Netiquette2.0.

Questi principi sono le linee guida fondamentali per la sicurezza e il benessere di tutti gli utenti della rete, in particolare negli ambienti usati dagli adolescenti o comunque da minorenni.

Tutti gli utenti della rete dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in materia di diritto d'autore e tutela della privacy nonché le specifiche norme civili e penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

Il curricolo scolastico prevede il regolare utilizzo della rete informatico-telematica sia per svolgere le normali attività didattiche inerenti i diversi corsi di studi attivati dall'IIS Lagrangia, sia in generale per trovare materiale, recuperare documenti e scambiare informazioni utilizzando le tecnologie per l'informazione e la comunicazione (TIC). In particolare Internet offre agli studenti e ai docenti una vasta scelta di risorse e di opportunità per lo studio anche attraverso il confronto e la condivisione di materiali.

L'IIS Lagrangia propone agli studenti e agli insegnanti di utilizzare Internet non soltanto, come potrebbe avvenire al di fuori del contesto scolastico, per le attività sociali o di intrattenimento e per il tempo libero, ma anche e soprattutto per promuovere il confronto e la condivisione delle risorse, l'innovazione e la comunicazione, nella convinzione che questi siano fattori che concorrono in modo significativo alla formazione della persona e del cittadino.

Accanto alle altre figure presenti in Istituto, i docenti e gli studenti sono gli attori primari del processo di insegnamento - apprendimento e per loro l'accesso ad Internet tramite la rete informatico-telematica dell'IIS Lagrangia, nel rispetto della **Politica per l'Uso Accettabile della Rete di Istituto** e delle disposizioni del Ministero dell'Istruzione Università e Ricerca, è un privilegio e un diritto.

Poiché esiste la possibilità di trovare su Internet materiale inadeguato ad un contesto scolastico ed educativo, quando non addirittura illegale, la Scuola ha assunto precauzioni in tal senso, tra le quali la limitazione dell'accesso al web mediante un filtro per la navigazione. Inoltre le attività svolte in rete vengono monitorate e tracciate nel rispetto delle vigenti normative sulla privacy. Il filtro da solo non è però in grado di eliminare tutti i rischi, anche perché è possibile commettere errori o attività illegali su siti perfettamente leciti. Per questo motivo tutti gli utenti che si trovino ad utilizzare la rete informatico-telematica dell'IIS Lagrangia hanno la responsabilità di agire con la dovuta prudenza e nel rispetto della legge.

Quindi tutti gli utenti della rete dell'IIS Lagrangia sono tenuti al rispetto:

- della legislazione vigente
- della Netiquette

ARTICOLO 2. L'importanza del discernimento dei rischi nella navigazione in rete

Le risorse nel mondo odierno non si trovano più solo in formato cartaceo, ma su diversi tipi di media, e comunque oramai quasi tutti digitali. Uno dei compiti della Scuola di oggi è fornire agli allievi sia un metodo di ricerca delle informazioni, sia un metodo di valutazione delle informazioni trovate.

In particolare gli insegnanti hanno la responsabilità di consigliare e guidare gli studenti nelle attività on-line e di stabilire obiettivi didattici chiari nell'uso di Internet, insegnando un uso dei nuovi strumenti di comunicazione che sia accettabile e responsabile nonché rispettoso dei valori morali, etici e della legalità.

L'IIS Lagrangia pone tra i suoi obiettivi formativi l'educazione dei propri allievi al discernimento rispetto all'accertamento dei rischi della navigazione web e alla valutazione dei contenuti di Internet. Gli studenti imparano ad utilizzare i metodi di ricerca su Internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Agli studenti viene anche insegnato che occorre valutare l'affidabilità delle fonti di informazione e a porsi rispetto ad esse in modo attento e critico.

Le abilità di gestione delle informazioni includono:

- il saper valutare le garanzia di validità, di diffusione e di origine delle informazioni a cui si accede o che si ricevono
- l'utilizzare fonti alternative di informazione per proposte comparate
- il rispettare i diritti d'autore e dei diritti di proprietà intellettuale

Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete e devono poter riconoscere ed evitare gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e l'intolleranza.
Tutte queste sono abilità che si acquisiscono con il tempo e sotto la guida dei docenti e l'IIS Lagrangia è determinato a fornire ai propri allievi una concreta opportunità formativa in tal senso.

ARTICOLO 3. Comportamenti corretti nelle relazioni informatico-telematiche

A - Principi generali delle relazioni sul web

1.
Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, devono essere considerati abusi da segnalare solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti sui quali semplicemente non ci si trova d'accordo.

2.
Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Netlog, ecc, bisogna informarsi subito su quali siano i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati ed esplorando i siti informativi e istituzionali che affrontano queste tematiche.

3.
Se si condividono informazioni personali, bisogna farlo con la dovuta attenzione:

- scegliendo con cura che cosa rendere pubblico e cosa rendere privato

- selezionando con prudenza le amicizie con cui accrescere la propria rete di conoscenze
- selezionando con prudenza i gruppi di discussione cui aderire
- proteggendo la propria identità digitale con password sufficientemente complesse e conservate con le dovute precauzioni
- utilizzando una domanda di recupero password dalla risposta non banale

4.
Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuarne la pubblicazione. Per esempio non bisogna pubblicare su YouTube video girati di nascosto o dove sono presenti persone che siano state filmate senza il loro esplicito consenso.
5.
Ogni abuso subito o rilevato nella navigazione web, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a serie conseguenze penali e giudiziarie.

B - Relazioni tra utenti di pari livello – (Rapporto 1 a 1)

6.
All'interno dei Social Network si instaurano relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. E' importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto, come numeri di telefono o indirizzi, che nella vita reale non si darebbero a persone che non godono della nostra fiducia.
7.
Bisogna evitare di scambiare file con utenti di cui non ci si può fidare e in ogni caso, anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine dei file ed effettuarne un controllo con un antivirus aggiornato.
8.
Se durante una chat, un forum o in una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando immediatamente la conversazione.
9.
Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata, per esempio un tentativo di approccio sessuale nonostante la minore età, stalking o Cyberbullismo, l'utente può sfruttare gli appositi sistemi di reportistica degli abusi predisposti all'interno del servizio, segnalando tempestivamente il nickname dell'utente che ha perpetrato l'abuso. In questi casi può essere conveniente abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento creandosene uno nuovo.
10.
Quando si facesse uso di sistemi di file-sharing P2P (e comunque mai a scuola) è importante evitare di scaricare dei file che possono essere considerati illegali e protetti dal diritto d'autore. Bisogna inoltre fare attenzione e non aprire mai file sospetti, verificandone prima la bontà con un

antivirus aggiornato; occorre ricordare che la maggior parte dei programmi P2P contiene spyware e malware, ovvero software malevoli in grado di compromettere seriamente la sicurezza del computer che si sta usando.
Per ovvi motivi di sicurezza della rete l'utilizzo questi sistemi a scuola è assolutamente vietato.

11.
I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica, quindi è necessario preservare la privacy di tutti

- cancellando il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscono tra loro
- evitando di inoltrare spam o cosiddette catene di Sant'Antonio
- perpetrando qualunque tipo di abuso per il mezzo dei messaggi elettronici

12.
Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo o immagini bisogna essere sicuri di averne il diritto d'uso e di non utilizzare alcun file coperto da copyright.

C - Contenuti generati dagli utenti e relativa visibilità – (Rapporto 1 a N)

13.
I contenuti pubblicati sulle applicazioni web dei Social Network, hanno diversi livelli di visibilità. Tra questi diversi livelli di visibilità citiamo:

- visibilità verso singolo utente
- visibilità verso gruppo di utenti
- visibilità pubblica ovvero verso tutti i potenziali utenti della rete

Tali differenti livelli di visibilità devono sempre essere tenuti a mente, dando a ciascun contributo pubblicato in rete l'appropriato livello di visibilità e quindi di privacy. Pertanto quando si inizia a pubblicare materiale in una community occorre utilizzare appropriatamente le funzioni per l'impostazione dei livelli di visibilità/ privacy.
14.
Teniamo sempre in dovuta considerazione che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare: bisogna quindi evitare a priori di contribuire con materiale che in futuro non si vorrebbe più veder pubblicato
15.
Quando si contribuisce con materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto dalla community, evitando di pubblicare materiale inadeguato o che potrebbe risultare fuori contesto: ci sono momenti e luoghi virtuali appropriati per parlare di qualsiasi tema nel rispetto degli interlocutori
16.
Se si usa un nuovo servizio messo a disposizione dal Social Network, bisogna informarsi su quali siano gli strumenti per segnalare materiale e comportamenti non idonei, e quali siano le modalità corrette per farlo
17.
Se un contenuto viene moderato e non è più visibile online, probabilmente è stato giudicato non idoneo dal moderatore. Verificare quindi il linguaggio che si era utilizzato e riesaminare se

l'ambiente dove lo si era pubblicato fosse stato davvero il posto migliore per quello specifico contenuto

18.

Quando si fa uso di etichette (TAG) per catalogare un contenuto/utente assicurarsi che il TAG sia coerente con il contenuto o che indichi la persona corretta; quando il TAG riguarda una persona sarebbe inoltre opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto espresso dal TAG.

D - La gestione delle relazioni sociali nelle comunità digitali – (Rapporto N a N)

19.

Le relazioni sociali che si sviluppano all'interno di un Social Network sono simili a quelle reali, per cui deve essere gestita la fiducia verso i propri contatti proprio come accade nella realtà. Bisogna aggiungere alla propria rete di amici solo le persone che hanno in vario modo dimostrato di essere affidabili, con cui si è a proprio agio e di cui abbiamo certezza rispetto alla loro reale identità. Occorre essere molto prudenti rispetto alla possibilità di aggiungere persone su cui si abbiano dubbi rispetto alla loro reale identità o che addirittura non si conoscano affatto.

20.

Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna evitare di condividere contatti e dati personali e contenuti privati, soprattutto se riguardano terze persone.

21.

La rete sociale non è facile da controllare quindi bisogna tenere sempre a mente che gli "amici degli amici" o gli amici di componenti del proprio "network" sono molti e spesso hanno modo, nonostante siano sconosciuti, di avere accesso alle nostre informazioni e ai nostri contenuti personali.

22.

Se si ha accesso alle comunicazioni private di altri utenti, per esempio perché l'utente ha impostato in maniera sbagliata i livelli di privacy, bisogna notificarlo all'utente ed evitare di leggere i messaggi privati.

23.

La reputazione digitale è persistente e si diffonde velocemente pertanto non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito.

ARTICOLO 4. UTILIZZO DI SMARTPHONE E TABLET

L'utilizzo di smartphone, tablet e altri dispositivi elettronici deve avvenire nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano, alla data attuale, l'uso in classe di telefoni cellulari e dispositivi elettronici
[Nota MIUR prot. n. 30 del 15/03/2007 con oggetto: ***Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti***]

L'IIS Lagrangia ha attivato, a partire dall'anno scolastico 2015/16 e su diverse classi, la sperimentazione "Classi3.0 - l'iPad nello zainetto". All'interno di queste classi tutti gli allievi dispongono di un iPad, o in comodato d'uso dalla Scuola o di proprietà personale.
In queste classi3.0 si utilizza un format didattico in cui gli allievi possono usare l'iPAD sia a scuola che a casa, a supporto ed integrazione dei tradizionali metodi d'insegnamento, che non vengono comunque abbandonati.

- Gli iPad acquistati dalla Scuola e ceduti in comodato d'uso agli allievi sono equipaggiati con le caratteristiche tecniche necessarie alla loro integrazione nella rete didattica di Istituto.
- Qualora le famiglie decidessero di acquistare autonomamente l'iPAD per il proprio/a figlio/a dovranno, comunque, rispettare le indicazioni tecniche indispensabili per l'integrazione nella rete didattica di Istituto: non potranno, infatti, essere integrati *device* di modello diverso o con caratteristiche non compatibili con lo standard stabilito dalla Scuola. Attraverso questa modalità operativa, gli studenti avranno a disposizione strumenti omogenei per la loro attività di studio, tutti parimenti controllabili ed inseribili nella rete didattica della classe. In ogni caso, per evidenti ragioni di sicurezza, anche i dispositivi personali saranno sottoposti a controllo nel momento in cui saranno collegati alla rete d'istituto.
- I dispositivi di proprietà della Scuola e forniti in comodato d'uso agli allievi dispongono della sola scheda di rete per la connessione WiFi.
- **Invece i dispositivi di proprietà dell'allievo potranno, in aggiunta e facoltativamente, disporre di una microscheda *cellular* per la connessione alla rete telefonica mobile, ma in tal caso è fatto espresso divieto di effettuare connessioni tramite tale modalità all'interno delle attività didattiche in Istituto.** E questo per ovvie ragioni: infatti quando ci si collega a Internet tramite iPAD in modalità WiFi e con la rete di Istituto, il filtro installato presso la Scuola blocca l'accesso a siti non appropriati, esattamente come un filtro blocca la navigazione dai computer fissi presenti nei locali scolastici. Durante le ore di lezione gli studenti lavorano sotto la supervisione degli insegnanti e con la protezione del filtro di navigazione. Una navigazione tramite microscheda *cellular* con connessione alla rete telefonica mobile sarebbe non coperta dal filtro dei contenuti e dai dispositivi di sicurezza dell'Istituto. Quando invece sono a casa gli allievi sono sotto la responsabilità della famiglia, che dovrà responsabilizzarli ad un corretto uso degli strumenti a loro disposizione.
- È compito della Scuola da un lato e della famiglia dall'altro educare a essere consapevoli dei rischi che si possono correre nell'utilizzo della rete e in particolare dei social network. La consapevolezza del pericolo è la prima forma di educazione.

ARTICOLO 5. Azioni di contrasto al cyberbullismo e altri fenomeni di rischio

Gli studenti, anche i più giovani, rappresentano spesso un'avanguardia tecnologica grazie alla loro capacità di utilizzare le opportunità offerte da smartphone, tablet e altri strumenti che consentono una costante connessione alla rete. Tuttavia alla capacità tecnologica non sempre corrisponde eguale maturità nel comprendere la necessità di difendere i propri diritti e quelli di altre persone, a partire dagli stessi amici e compagni di studio. Gli studenti devono essere consapevoli che le proprie azioni in rete possono produrre effetti negativi tangibili anche nella vita reale e per un tempo indefinito. Troppi ragazzi, insultati, discriminati, vittime di cyberbullismo, soffrono e possono essere costretti a cambiare scuola o, nei casi più tragici, arrivare al suicidio. È quindi estremamente importante prestare attenzione in caso si notino comportamenti anomali e fastidiosi sui social network, su sistemi di messaggistica istantanea (come Whatsapp, Snapchat, Skype, Messenger, etc.) o su siti che garantiscono comunicazioni anonime. Se si è vittime di commenti odiosi, di cyberbullismo, di sexting o di altre ingerenze nella propria vita privata, non bisogna aspettare che la situazione degeneri ulteriormente. Se ci si rende conto che qualcuno è insultato o messo sotto pressione da compagni o da sconosciuti occorre avvisare subito i docenti e le famiglie. Si può chiedere al gestore del social network di intervenire contro eventuali abusi o di cancellare testi e immagini inappropriate. In caso di violazioni, è bene segnalare immediatamente il problema alla propria Istituzione Scolastica che valuterà gli estremi per una segnalazione al Garante della Privacy e alle autorità competenti.

ARTICOLO 6. Possibili reati e violazioni della legge in rete

Al di là delle regole di buona educazione e di Netiquette ci sono comportamenti in rete, solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti da parte dell'autorità giudiziaria con conseguenze anche serie. E' nostro dovere ricordarli in questo documento, per evidenziare come anche strumenti hardware o software con ottime potenzialità didattiche possano dar luogo, in caso di uso improprio, a comportamenti perseguibili sia penalmente che civilmente.
Eccone alcuni.

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

La legge 547/93 individua e vieta tutta una serie di comportamenti nell'ambito informatico che si reputano lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:

- Accesso abusivo ad un sistema informatico e telematico
  - Attività di introduzione in un sistema, a prescindere dal superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo. [Art. 615 ter cp]
  - 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 cui non siamo autorizzati.
- 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.
  - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. **In particolare si ricorda che l'accesso alla rete attraverso**

autenticazione con credenziali trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.
Si ricorda pertanto che ogni utente accreditato sulla rete dell'IIS Lagrangia è tenuto a conservare in modo scrupoloso le proprie credenziali di accesso alla rete stessa non comunicandole ad altre persone.

  - E' considerato reato anche quando l'informazione viene fraudolentemente carpita 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 solo per scherzo, i codici di accesso alla posta elettronica, al Messenger o al profilo di amici, compagni, colleghi o comunque terze persone.
- Frode informatica
  - Questo delitto 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 il danneggiamento informatico in conseguenza alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o alla 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 digitale, telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.
- Diffamazione
  - Chiunque 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]
  - Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito web o su un 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, anche per via telematica. [Art. 612 cp]
- Può capitare che 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" anche 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 159/93 sottolinea all'art. 1 che viola i diritti d'autore 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, che siano protette dalla legge 22 aprile 1941, n. 633 e successive modificazioni, ovvero pone in commercio, detiene per la vendita o introduce a fini di lucro le copie.
  - 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 o utilizzare immagini soggette a copyright.
  - 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 o smarrimento della copia originale. 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.