Disciplinare per l'Uso Accettabile della Rete: *internet, posta elettronica e postazioni multimediali*

(Linee guida del Garante per la posta elettronica e Internet, G. U. n° 58 del 10-03-2007, Reg. Delib. n° 13 del 01 marzo 2007)

(*Delibera C.d.I. n.11 del 23 settembre 2013*)

INDICE

PREMESSA

Il POF promuove l'informatizzazione dell'Istituto e prevede il regolare utilizzo dei computer installati nei laboratori, nelle aule e in tutti i locali adibiti ad ufficio o a disposizione dei docenti per attività inerenti la loro funzione. Con i computer gli studenti, oltre a svolgere le normali attività tecniche previste dai curricoli scolastici, hanno modo di produrre e trovare materiali, salvare, recuperare e scambiare documenti e informazioni in genere utilizzando le Tecnologie per l'Informazione e la Comunicazione (TIC).
In particolare internet offre agli studenti e ai docenti la possibilità di trovare risorse e l'opportunità di pubblicazione e di scambio.

La scuola italiana propone agli studenti e ai docenti di utilizzare internet non soltanto per le attività sociali, ma anche per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per i docenti l'accesso ad internet a scuola, nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano l'uso in classe di telefoni cellulari e dispositivi elettronici, è un'opportunità e un diritto.

Al fine di evitare l'utilizzo di materiale inadeguato e illegale, che facilmente si può trovare in internet, l'istituto ne ha limitato l'accesso attraverso un sistema di filtri per la navigazione implementati sul firewall hardware della rete. Tutte le attività svolte in rete vengono monitorate e tracciate nel rispetto delle normative vigenti in materia di privacy. Nonostante questi accorgimenti, non può essere escluso il rischio che gli studenti, per errore o coscientemente, utilizzino materiale inadeguato o svolgano attività illegali anche su siti perfettamente leciti, soprattutto quando sono autorizzati all'uso di dispositivi elettronici personali di memoria o telefonici con collegamento autonomo ad internet.
Per questo motivo:

- i docenti hanno la responsabilità di guidare e controllare gli studenti nelle attività on-line in istituto, stabilendo obiettivi chiari nell'uso di internet e insegnando un uso dei nuovi strumenti di comunicazione accettabile e responsabile;
- i genitori hanno il dovere di vigilare sull'uso del computer e dei dispositivi di comunicazione da parte dei propri figli, sia casa, che nel tempo libero, ricordando le regole per una navigazione sicura in internet e chiedendo che esse siano rispettate.

Il presente Disciplinare per l'Uso Accettabile della Rete fornisce le linee guida e stabilisce le regole dell'istituto per il benessere e la sicurezza di tutti gli utenti della rete. Esso viene diffusa all'interno e reso disponibile sul sito dell'istituto.
Tutti gli utenti della rete dell'istituto devono rispettare scrupolosamente le regole qui stabilite, le leggi vigenti in materia di diritto d'autore e tutela della privacy, nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

TITOLO 1 - Comportamento in rete

Fra gli utenti dei servizi telematici Internet, si sono sviluppati nel corso del tempo una serie di principi di buon comportamento che vengono identificati con il nome di Netiquette.
Questi principi sono le linee guida fondamentali per la sicurezza e il benessere di tutti nella rete, in particolare negli ambienti più usati dagli adolescenti.
Tutti gli utenti della rete dell'istituto devono rispettare scrupolosamente questi principi, che di seguito si riportano.

1.1. - Principi Generali

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, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.
2. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Netlog, etc…, bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche (ad esempio www.tiseiconnesso.it).
3. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato, scegliendo con cura le amicizie con cui accrescere la propria rete e i gruppi a cui aderire e proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale (evitare nomi del proprio cane, gatto, ecc…).
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 bisogna pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
5. Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.
6. Ogni abuso subito o rilevato nella navigazione, 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 conseguenze penali e giudiziarie che possono durare anni.

1.2. - Comportamenti nelle relazioni tra persone di pari livello (rapporto 1 a 1)

1. All'interno dei Social Network si instaurano tante 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 sono ancora degne di fiducia.
2. 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.
3. 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 la conversazione.
4. 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 del predisposti all'interno del servizio, segnalando tempestivamente il nickname 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.
5. Quando si fa uso di sistemi di file-sharing P2P, 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 dei file sospetti, verificandone la bontà con un antivirus aggiornato. La maggior parte dei programmi P2P contiene spyware e malware, software malevoli in grado di compromettere seriamente la sicurezza del computer che si sta usando. Per motivi di sicurezza della rete l'utilizzo questi sistemi a scuola è vietato.
6. 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, evitare di inoltrare spam o catene di sant'Antonio, o perpetrare qualunque tipo di abuso usando i messaggi elettronici.
7. 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 alcun file coperto da copyright.

1.3. - Creazione e diffusione di contenuti generati dagli utenti (rapporto 1 a N)

1. I contenuti pubblicati sulle applicazioni web dei Social Network, hanno diversi livelli di visibilità, per esempio singoli utenti o tutti gli utenti della rete, che devono sempre essere tenuti a mente, dando a ciascun contributo i corretti livelli di privacy. Pertanto, quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy.
2. Dal momento che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.
3. Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori

contesto: ci sono momenti e luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori.
4. Se si usa un nuovo servizio messo a disposizione dal Social Network, bisogna informarsi su quali sono gli strumenti per segnalare materiale e comportamenti non idonei, e quali sono le modalità corrette per farlo.
5. Se un contenuto viene moderato e non è più visibile online, probabilmente è non idoneo. Modificare linguaggio e controllare se il punto dove lo si è pubblicato è davvero il posto migliore per quello specifico contenuto.
6. Quando si fa uso di etichette per catalogare un contenuto/utente (TAG), bisogna assicurarsi che 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.

1.4. - Gestione delle relazioni sociali – *Communities* (rapporto N a N)

1. Le relazioni sociali che si sviluppano all'interno di un Social Network sono simili a quelle reali: 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 vari modi dimostrato di essere affidabili, con cui si è a proprio agio e di cui siamo a conoscenza della reale identità. Inoltre conviene gestire la propria privacy quando si aggiungono persone su cui si hanno dubbi o non si conoscono affatto.
2. 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.
3. La rete sociale non è facile da controllare quindi bisogna tenere sempre a mente che gli "amici degli amici" o di componenti del proprio "network" sono molti e spesso hanno modo, nonostante siano sconosciuti, di avere accesso alle informazioni e ai contenuti personali.
4. 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.
5. 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.

TITOLO 2 – Sicurezza e Uso delle TIC

2.1. - Rete di Istituto e postazioni informatiche

Al fine di garantire una gestione il più possibile corretta delle dotazioni informatiche, l'istituto attua le seguenti misure:
1. Limita l'accesso e l'uso della rete interna ed esterna (internet) secondo i normali canali di protezione presenti nei sistemi operativi e utilizza un firewall hardware di rete con funzioni di antivirus, antispyware, antispam, prevenzione delle intrusioni e web filter, configurato in base alle necessità di accesso stabilite dagli OO.CC. e nel rispetto delle condizioni operative di

sicurezza del CED e della rete stabilite dal dirigente e dall'amministratore di sistema. In ogni caso il filtro sui contenuti web deve evitare l'accesso a siti con contenuto illegale, violento, pedo-pornografico, razzista o non conforme alla policy adottata. Nei laboratori, ove sussiste una rete locale collegata alla rete di istituto, l'accesso a internet dalle postazioni degli studenti è consentito o meno in automatico dal docente in servizio. Tutte le postazioni informatiche, qualora non utilizzano sistemi operativi Linux, sono protette da antivirus.

2. L'utilizzo di ogni postazione informatica di cui è dotato l'istituto prevede l'autenticazione con credenziali personali rilasciate, per il personale docente e ATA, all'atto di presa in servizio e, per gli studenti, alla prima iscrizione. L'istituto traccia e archivia tutto il traffico della rete interna ed esterna, nel rispetto delle disposizioni di legge vigenti in materia e ad esclusiva disposizione dell'Autorità giudiziaria. Monitora costantemente l'efficienza del proprio sistema informatico attraverso software dedicati in modalità ASP. A livello di laboratorio, aula o ufficio, i docenti con funzioni di responsabilità nella conduzione dei reparti e gli assistenti tecnici controllano periodicamente il buon funzionamento delle postazioni informatiche, del sistema operativo, del software applicativo e di sicurezza installati. L'utilizzo di CD, DVD, chiavi o dispositivi di storage USB e floppy personali è autorizzato dal docente in servizio. Nei locali della scuola, durante la lezione o dell'attività, previa richiesta del docente e solo per fini didattici, il dirigente può autorizzare gli studenti all'uso di computer, tablet o smartphone personali, anche con collegamento a internet autonomo o attraverso la rete di istituto. In questo caso, comunque, sono rispettate le condizioni operative e di sicurezza stabilite dall'amministratore di sistema.
3. Gestisce l'accesso alla propria rete wireless a mezzo controller. Essa è prevalentemente dedicata all'uso del registro elettronico in classe e al collegamento ad internet delle aule e dei locali non serviti dalla rete LAN. Il collegamento di apparecchiature personali a tale rete è autorizzato dal dirigente, tenuto conto delle condizioni operative e di sicurezza stabilite dall'amministratore di sistema ed è vincolato ad autenticazione con la tecnica captive portal. Il servizio di accesso alla rete wireless è regolamentato da specifico "Regolamento di utilizzo e codice di comportamento".
4. Al fine di evitare comportamenti impropri o illeciti, introduce divieti o limitazioni attraverso i propri regolamenti o direttive dirigenziali in materia di:
   - download di file video-musicali protetti da copyright;
   - download, installazione nei computer o utilizzo di software non autorizzati;
   - navigazione in siti non necessari ad una normale attività didattica o non accettati dalla protezione interna alla scuola;
   - alterazione dei parametri di protezione dei computer in uso;
   - divieto di svolgere ogni attività che possa eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi a rendere inefficaci schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet;
   - utilizzazione della rete per interessi privati e personali;

- non rispetto delle leggi sui diritti d'autore.

2.2. - Utilizzo dei servizi Internet

I servizi internet offerti dall'istituto sono utilizzabili dal personale docente e ATA, dagli studenti e dai loro genitori e da eventuali ospiti autorizzati secondo le seguenti disposizioni:

- il docente, che nella propria programmazione prevede l'utilizzo di internet, è responsabile di quanto avviene nelle proprie ore di lezione, sia in laboratorio, che in aula;
- previa richiesta all'amministratore di sistema, possono essere assegnati a docenti, personale non docente, classi, gruppi o progetti, eventuali indirizzi email nel dominio di Istituto "istitutoeinstein.net";
- l'utilizzo delle caselle email nel dominio "istitutoeinstein.net" è legato al solo ambito amministrativo, organizzativo e didattico;
- è vietato utilizzare email personali ad uso privato durante le ore di lezione;
- è vietato l'utilizzo delle postazioni durante le ore di lezione per motivi non strettamente legati alla pratica didattica o a esigenze amministrative o organizzative;
- su richiesta del docente è permessa la partecipazione a forum nell'ambito dei siti ammessi;
- gli studenti non possono usare i computer dell'istituto in rete internet senza l'autorizzazione e il coordinamento del docente; eventuali inadempienze da parte degli studenti avranno riflessi sulla valutazione della condotta e potranno comportare sanzioni disciplinari secondo quanto stabilito dal Regolamento di Istituto;
- è vietato a tutti il download a fini personali di file musicali, foto, software, video, ecc., tranne nel caso di specifiche attività didattiche preventivamente programmate.

TITOLO 3 - Linee guida di utilizzo delle TIC per Studenti, Docenti e ATA

3.1. - Studenti

Gli studenti sono tenuti a:

- non utilizzare giochi né in locale, né in rete;
- salvare i lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione locale o di rete secondo le disposizioni impartite dal docente o dal responsabile di laboratorio;
- in caso di utilizzo di internet, mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo dell'istituto;
- non inviare fotografie personali o di amici;
- non caricare, scaricare o copiare materiale da internet senza il permesso del docente o del responsabile di laboratorio.

3.2. - Docenti

I docenti sono tenuti a:

- utilizzare le postazioni informatiche solo per ragioni inerenti il proprio lavoro o riconducibili alla propria funzione;
- non lasciare le e-mail o file personali sui computer o sul server dell'istituto;
- salvare i lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete locale o d'istituto, evitando l'utilizzo del desktop;
- fare il logout al termine dell'uso di applicativi che richiedono credenziali di accesso o di una sessione di internet e spegnere il computer alla fine della sessione di lavoro;
- discutere con gli studenti del Disciplinare per l'Uso Accettabile della Rete dell'istituto e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di internet;
- dare chiare indicazioni su come si utilizza internet, ed eventualmente anche la posta elettronica, e informarli che le navigazioni saranno monitorate;
- ricordare di verificare lo stato dei computer alla fine della sessione di lavoro, in particolare controllando che siano spenti all'uscita dall'ultima ora di lezione;
- ricordare agli studenti che la violazione consapevole della Politiche qui contenute può comportare l'avvio di procedimenti disciplinari a loro carico secondo quanto stabilito dal regolamento d'istituto, nonché, in caso di dolo accertato, danno luogo a richiesta di risarcimento per le spese di ripristino del sistema sostenute dalla scuola, ferme restando possibili azioni legali in sede civile e la denuncia del reato all'autorità giudiziaria;
- segnalare alla dirigenza eventuali comportamenti non corretti o abusi nell'uso delle apparecchiature informatiche e nella fruizione della rete di istituto;
- non dimenticare mai che nel caso di infrazione consapevole da parte del docente, sarà compito del dirigente scolastico intervenire per via amministrativa secondo le norme vigenti e, in ipotesi di reato, trasmettere la denuncia all'autorità giudiziaria.

3.3. – Personale ATA

Il personale ATA è tenuto a:

- utilizzare le postazioni informatiche solo per ragioni inerenti il proprio lavoro o riconducibili alla propria funzione;
- non lasciare le email o file personali sui computer o sul server dell'istituto;
- salvare i lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete locale o d'istituto, evitando l'utilizzo del desktop;
- fare il logout al termine dell'uso di applicativi che richiedono credenziali di accesso o di una sessione di internet e spegnere il computer alla fine della sessione di lavoro;
- collaborare con i docenti sulla diffusione di comportamenti da parte di studenti e ospiti rispettosi del Disciplinare per l'Uso Accettabile della Rete dell'istituto;
- segnalare ai docenti responsabili di laboratorio o alla dirigenza eventuali comportamenti non corretti o abusi nell'uso delle apparecchiature informatiche e nella fruizione della rete di istituto;
- non dimenticare mai che nel caso di infrazione consapevole da parte del medesimo personale, sarà compito del dirigente scolastico intervenire per via

amministrativa secondo le norme vigenti e, in ipotesi di reato, trasmettere la denuncia all'autorità giudiziaria.

3.4. - Sito web dell'Istituto e servizi on-line

L'istituto dispone di un proprio sito web e di un proprio dominio: www.istitutoeinstein.net.
L'istituto gestisce il proprio sito attraverso un servizio di hosting.
L'istituto detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.
L'istituto, in qualità di ente pubblico, pubblica sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.
L'istituto offre all'interno del proprio sito web i seguenti servizi agli studenti, alle famiglie ed agli utenti esterni:

- informazioni sull'istituto e la sua organizzazione;
- informazioni sull'Offerta Formativa e Orientamento scolastico;
- informazioni sull'amministrazione dell'Istituto e sui progetti attivati;
- l'albo pretorio on-line;
- consultazione di avvisi e comunicazioni;
- consultazione di regolamenti, POF, contratto decentrato di istituto, norme disciplinari e codice di comportamento dei pubblici dipendenti;
- modulistica;
- link per l'accesso al registro elettronico da parte di studenti, genitori e docenti;
- link a siti di interesse per la propria utenza.

3.5. – Utilizzo di cellulari, di smartphone e di apparecchi di comunicazione in genere

Agli studenti non è permesso utilizzare i telefoni cellulari, gli smartphone o altri apparecchi di comunicazione per telefonare, inviare sms, scattare foto o registrare filmati durante l'orario scolastico, ad eccezione della ricreazione.
Ai docenti ed al personale, che entra in diretto contatto con gli studenti, è vietato l'uso del telefono cellulare durante lo svolgimento delle lezioni, fatti salvi casi di forza maggiore.
Ai docenti ed al personale, che entra in diretto contatto con gli studenti durante lo svolgimento delle lezioni, è consentito l'uso di smartphone o tablet con collegamento autonomo a internet esclusivamente per ragioni didattiche.

TITOLO 4 - Informazione

4.1. - Informazione del personale scolastico

Il personale scolastico (docente ed ATA) prende visione e sottoscrive il presente documento all'inizio del rapporto di lavoro ed ogni qualvolta vi sarà apportata una variazione.

4.2. - Informazione degli studenti

E'cura del docente responsabile del laboratorio e dei docenti che intendono utilizzare le tecnologie informatiche in aula illustrare agli studenti i contenuti del Disciplinare per l'Uso Accettabile della Rete e delle TIC, evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica.

4.3 - Informazione dei genitori/tutori

I genitori saranno informati sul Disciplinare per l'Uso Accettabile della Rete e delle TIC nell'istituto e sulle regole da seguire a casa tramite:

- esposizione del seguente documento all'albo;
- pubblicazione dello stesso sul sito web della scuola;
- consultazione del documento in segreteria.

All'atto della prima iscrizione è fatto firmare al genitore/tutore dello studente un documento che attesta la conoscenza dell'esistenza del Disciplinare, la possibilità di consultarlo e le responsabilità dello studente sull'utilizzo delle risorse informatiche all'interno dei laboratori e delle aule. L'istituto chiede ai genitori degli studenti minori di 18 anni di età il consenso all'uso di Internet per il loro figlio e per la pubblicazione dei suoi lavori e della sue fotografie per finalità didattiche.

TITOLO 5 – Sanzioni

La violazione delle regole stabilite dal presente Disciplinare o il dolo accertati, qualora siano a carico dello studente, oltre all'intervento disciplinare del consiglio di classe, daranno luogo alla richiesta di risarcimento dei danni subiti comprese le ore di lavoro impiegate dal personale interno per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque salve ulteriori azioni civili, nonché l'eventuale denuncia del reato all'autorità giudiziaria. Nel caso di infrazione consapevole da parte dei docenti o del personale non docente sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti e, in ipotesi di reato, trasmettere la denuncia all'autorità giudiziaria.

TITOLO 6 - Disposizioni di legge e sanzioni

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e

propri reati e, conseguentemente, a subire procedimenti penali dalle conseguenze molto serie. A titolo di esempio, si riportano di seguito alcuni reati e violazioni di legge in cui è possibili incorrere.

6.1. - Reati informatici

La legge 547/93 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 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 su 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 eliminare le protezioni di 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 carpita in modo fraudolento 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 e compagni.
- 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 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.

6.2. - 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
  - Qualcuno che 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 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 online, 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 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 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.