Liceo Scientifico Statale
Albert Einstein

Via A. Einstein,3
20137Milano

www.liceoeinsteinmilano.edu.it

Tel 02.5413161
Fax 02.5460852

didattica@liceoeinsteinmilano.edu.it
amministrativa@liceoeinsteinmilano.edu.it
mips01000g@istruzione.it
mips01000g@pec.istruzione.it

C.F.
80125710154

C.M.
MIPS01000G

IL CONSIGLIO DI ISTITUTO

VISTA la L. 135/2012, del 07/08/2012, "Conversione in legge, con modificazioni, del decreto---legge 6/07/2012, n. 95, recante disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini";

VISTA la L. 633/1941, Testo consolidato al 09/02/2008, "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";

VISTO il D.Lgs. 305/2006 del 07/12/2006, "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione", in attuazione degli articoli 20 e 21 del D.Lgs. 30/06/2003, n. 196, "Codice in materia di protezione dei dati personali";

VISTA la L. 4/2004, "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici";

VISTO il D.Lgs 196/2003 Testo Unico sulla privacy entrato in vigore il 01/01/2004 che riassume le norme precedenti sulla privacy;

VISTO il D.Lgs 68/2003, "Sulla regolamentazione per la tutela del diritto d'autore e dei diritti connessi nella società dell'informazione";

VISTA la L. 325/2000, "Sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'art.15 della Legge 675/1996";

VISTA la L. 248/2000, "Nuove norme di tutela del diritto d'autore";

VISTO il D.P.R. n. 275 del 25/02/1999, "Regolamento recante norme in materia di autonomia delle istituzioni scolastiche", ai sensi dell'art. 21 della legge 15/03/1997, n. 5;

VISTA la L. 547/1993, "Norme in materia di reati informatici".

VISTA la C.M. 114/2002, "Sulle infrastrutture tecnologiche nelle scuole e nuove modalità di accesso al sistema informativo";

VISTA la C.M. 152/2001, "Sulla diffusione delle reti LAN";

VISTE le "Linee guida per i siti web della PA", del 26/07/2010;

CONSIDERATO il comunicato stampa del Garante per la protezione dei dati personali, "La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare", del 06/09/2012;

TENUTO CONTO della "Nota informativa sul trattamento dei dati personali", ai sensi della L. 675/96 e s.m. e i. ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") che è parte integrante del regolamento interno sottoscritto dai genitori o da chi ne fa le veci all'atto della consegna del libretto delle comunicazioni scuola-famiglia della Scuola,

con propria delibera nella seduta del 7.09.2020

ADOTTA

il seguente Regolamento relativo alla "Politica d'uso accettabile e sicuro della rete e Regolamento di accesso e utilizzo delle risorse tecnologiche" (di seguito: PUA).

§1. PREMESSA

È ormai prassi comune che a scuola ci si connetta al vasto mondo di Internet sia per svolgere significative esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative. Nello stesso tempo non si può ignorare che Internet sia anche una potenziale fonte di rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usarla e alla consapevolezza delle funzioni che la Rete rende possibili. Stesso discorso deve oggi essere fatto per il complesso sistema di computer in rete presenti nella scuola, sia riguardo ai tradizionali laboratori, sia riguardo agli uffici amministrativi e più in generale alle aule singole o specifiche predisposte per il collegamento interno ed esterno.

Il presente Regolamento intende dare un impulso allo sviluppo di una cultura d'uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi opportune per un uso sempre più professionale da parte di tutto il personale.

Il presente Regolamento, con cui l'Istituto si dota di una "Politica d'uso accettabile" (PUA) in materia di "Tecnologie dell'Informazione e della Comunicazione" (TIC), sarà portato a conoscenza di genitori, studenti e personale scolastico.

Il Regolamento non fa riferimento solo ai pericoli presenti in Internet, ma anche alla rete interna dell'Istituto, il cui uso improprio può generare problemi da un punto di vista didattico, nonché difficoltà di uso delle attrezzature, fino al blocco delle stesse, comportando un danno funzionale ed anche economico. Inoltre, poiché non è sempre chiaro quali siano le responsabilità in caso di conseguenze civili e penali, che comunque esistono, derivanti dall'uso improprio delle TIC, è importante e prioritario definire all'interno dell'Istituzione scolastica delle regole chiare che pongano le basi per lavorare serenamente, sicuri di aver messo in atto quanto possibile in chiave di prevenzione, ma soprattutto per usare in modo efficiente e didatticamente costruttivo le suddette tecnologie.

Nel documento che definisce la PUA d'Istituto vengono date indicazioni in merito a:

- accesso alle postazioni in rete della scuola dei diversi soggetti operanti nell'Istituto: personale in servizio, allievi, eventuali soggetti esterni alla scuola;
- accesso ai servizi resi disponibili sui computer in rete dei diversi soggetti operanti nell'Istituto;
- garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto.

Vengono inoltre predisposti strumenti hardware e/o software da impiegare per evitare o ridurre al minimo:

- l'uso improprio dell'accesso a Internet, in particolare riguardo alla gestione relativa al traffico generato sulla LAN in uscita e in entrata verso Internet;
- i danni causati da virus o da software che viola le norme sopra definite;
- il rischio di intrusioni indesiderate dall'esterno della LAN;
- i tempi di recupero della piena funzionalità dell'infrastruttura

§2. COMPORTAMENTI

§2.1 Comportamento in rete e uso consapevole delle tecnologie

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. Con l'avvento del web 2.0 e dei Social Network, basati sui principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti, dando vita ad un galateo del web2.0 che prende il nome di Netiquette 2.0.

Questi principi rappresentano le basi 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, 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.

§2.2 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 (YouTube, Facebook, Netlog, ecc…), 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.
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.
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 registrare né condividere, direttamente o indirettamente, su alcun sito web, applicazione o piattaforma multimediale, contenuti audio/video senza l'autorizzazione delle persone filmate o registrate.
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.

§2.3 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 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.

§2.4 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 vedere 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.

§2.5 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.

§3. SICUREZZA E USO DELLE TIC

§3.1 Rete di Istituto, servizi e postazioni informatiche

Al fine ridurre i rischi derivanti dall'usi della rete e dei dispositivi informatici, la scuola attiva le seguenti procedure:

- il sistema informatico è periodicamente controllato dai responsabili;
- la scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina;
- la scuola archivia i tracciati del traffico Internet (log del software proxy principale);
- è vietato scaricare da Internet software non autorizzati;
- le postazioni pc in ambiente Windows sono protette da software che impedisce modifiche ai dati memorizzati sul disco fisso interno;
- al termine di ogni collegamento la connessione deve essere chiusa;
- verifiche antivirus vengono condotte periodicamente sui computer e sulle unità di memorizzazione di rete;
- l'utilizzo di CD, chiavi USB e floppy personali deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto;
- la scuola si riserva di limitare il numero di siti visitabili e le operazioni di download;
- il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

§3.2 Accertamento dei rischi e valutazione dei contenuti di Internet

Il sistema di accesso ad Internet della scuola prevede l'uso di un filtro sui contenuti per evitare l'accesso a siti web con contenuto illegale, violento, pedo-pornografico, razzista o comunque non conforme alla policy adottata. In particolare il sistema tende a:

- impedire l'accesso a siti non appropriati;
- monitorare e tracciare i collegamenti di ogni utente;
- regolamentare l'utilizzo di risorse online quali chat, mail e forum.

§3.3 Utilizzo dei servizi Internet

La responsabilità del docente prevista dalla vigente normativa in materia di vigilanza si estende alle ore di lezione tenute nel laboratorio informatico.

Allo studente è fatto divieto di utilizzare e-mail personali ad uso privato durante le ore di lezione, di usare dispositivi informatici dell'Istituto o personali, nella rete internet, senza l'ausilio e il coordinamento del docente, di scaricare a fini personali file musicali, foto, software, video, ecc., tranne nel caso di specifiche attività didattiche preventivamente programmate.

§3.4 Sicurezza della rete interna (LAN)

L'Istituto dispone di un dominio su rete locale cui accedono i computer dell'amministrazione, tali postazioni sono su una rete locale isolata dal resto della rete di Istituto. Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico; è prevista la fornitura del servizio DHCP per l'assegnazione automatica di un indirizzo di rete.

La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati.

Sui dispositivi (PC) collegati alla rete LAN didattica non è garantito alcun servizio di backup, pertanto è opportuno fare copia su un supporto personale dei propri dati.

§3.5 Sicurezza della rete senza fili (Wireless – WiFi)

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un server che determina l'accesso degli utenti dietro richiesta di credenziali (nome utente e password).

L'ottenimento delle credenziali è riservato a studenti e personale dell'Istituto, sottoscrizione di apposito modulo/dichiarazione, da richiedere al Dirigente Scolastico. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

§4. LINEE GUIDA DI UTILIZZO DELLE TIC

§4.1 Indicazioni operative per gli studenti

- Non utilizzare giochi né in locale, né in rete;
- salvare sempre i lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni e non in posizioni sull'hard disk locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;
- mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della vostra scuola;
- non inviare a nessuno fotografie personali o di amici;
- chiedere sempre all'insegnante o al personale tecnico il permesso di scaricare documenti da Internet;
- chiedere sempre il permesso prima di iscriversi a concorsi o prima di riferire l'indirizzo della vostra scuola;
- riferire all'insegnante se qualcuno invia immagini che infastidiscono e non rispondere;
- riferire all'insegnante se capita di trovare immagini di questo tipo su Internet o se qualcuno su Internet chiede un incontro di persona;
- ricordarsi che le persone che incontrate nella rete sono estranei e non sempre sono quello che dicono di essere;
- non inviare mail personali, rivolgersi sempre all'insegnante prima di inviare messaggi di classe;
- non caricare o copiare materiale da Internet senza il permesso dell'insegnante o del responsabile di laboratorio.

§4.2 Indicazioni operative per i docenti

- Evitare di lasciare le e-mail o file personali sui computer o sul server della scuola;
- salvare sempre i lavori in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni e non sull'hard disk locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;
- discutere con gli alunni della PUA della scuola 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 informare che le navigazioni saranno monitorate;
- ricordare di verificare lo stato dei computer alla fine della sessione di lavoro, in particolare controllando che siano tutti spenti all'uscita dall'ultima ora di lezione;
- ricordare agli alunni che la violazione consapevole della PUA della scuola costituisce comportamento antidoveroso, passibile di sanzione disciplinare da parte del Consiglio di classe secondo le previsioni del Regolamento di Istituto.

§5. INFORMAZIONE SULLA POLITICA D'USO ACCETTABILE DELLE TIC DELLA SCUOLA

§5.1 Informazione al personale scolastico

Le regole di base relative all'accesso ad Internet sono pubblicate sul sito, esposte all'albo dell'Istituto, all'interno dei laboratori di informatica e negli uffici amministrativi.
Il personale scolastico (docente ed ATA) è tenuto alla conoscenza e al rispetto di quanto previsto nel presente Regolamento.

§5.2 Informazione agli studenti

Sarà cura del docente responsabile del laboratorio e dei vari docenti utenti del medesimo illustrare i contenuti della Politica d'Uso Accettabile delle TIC agli allievi, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica.

§5.3 Informazione ai genitori/tutori

I genitori saranno informati sulla politica d'uso accettabile e responsabile di Internet nella scuola e sulle regole da seguire a casa tramite:

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

§6. SITO WEB DELL'ISTITUTO

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.liceoeinsteinmilano.edu.it
L'Istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola 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.
La scuola, in qualità di ente pubblico, pubblicherà 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.

§7. SANZIONI

La violazione delle disposizioni di cui al presente Regolamento costituisce comportamento antidoveroso ed è passibile di sanzione disciplinare da parte del Consiglio di classe secondo quanto previsto dal Regolamento di Istituto, al quale si rimanda.
Tutti gli eventuali oneri conseguenti alla necessità di ripristinare il sistema informatico della scuola saranno a carico dei responsabili del danno.

APPENDICE: Disposizioni di legge e sanzioni

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 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, 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
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 terzi.

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.

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.