REGOLAMENTO PER L'UTILIZZO DEI DISPOSITIVI INFORMATICI FISSI E MOBILI, PER L'ACCESSO ED USO DELLA RETE INFORMATICA E DI INTERNET

PREMESSA E PRINCIPI GENERALI

L'attenzione all'attività didattica è un processo che coinvolge sì gli strumenti di apprendimento, come quelli tecnologici, ma soprattutto è rivolta alla libertà del singolo destinatario di detta attività formativa, e quindi deve essere quotidianamente modellata e riconfigurata da parte di ciascun soggetto, docente o alunno che sia, in modo tale che la motivazione all'apprendimento, ed alla sua offerta, possa rappresentare un obiettivo verso il quale tendere affinché l'intera attività didattica compia nel modo migliore il suo ruolo principale.

Da questo punto di vista, l'uso della tecnologia informatica nella scuola è una risorsa:

- gli strumenti tecnologici facilitano l'apprendimento, lo arricchiscono e rappresentano il tramite con il mondo di oggi. Tuttavia è ancora relativamente breve, sia per i docenti sia per gli alunni, il tempo trascorso dall'introduzione ed utilizzo di tali strumenti nella didattica, perché si sia consolidata una base legislativa ed una solida cultura etica e comportamentale tali da fornire autonomamente soluzioni e strategie risolutive.
- La progressiva diffusione e sviluppo delle nuove tecnologie informatiche ed il sempre più libero accesso alla rete Internet espone gli istituti scolastici, e gli utenti che in essa vi operano, a rischi di natura patrimoniale ed a responsabilità civili e penali derivanti da violazioni di specifiche norme di legge, potendo insorgere evidenti problemi in ordine alla sicurezza ed all'immagine degli istituti stessi.

L'Istituto Statale di Istruzione Superiore "C. Facchinetti" di Castellanza - VA, di seguito denominato anche Istituto, ritiene pertanto di dotarsi di un Regolamento Interno per l'utilizzo di tali risorse tecnologiche ed informatiche per uno svolgimento proficuo, ma anche sicuro, dei propri compiti istituzionali, al fine di tutelare in ogni forma e modo, non solo l'Istituto medesimo, ma anche tutti coloro che agiscono a qualsiasi titolo al suo interno.

L'Istituto si impegna a fornire, nelle forme e modalità che saranno ritenute più idonee dai propri organi collegiali, momenti e/o incontri formativi e informativi rivolti a tutto il personale docente, non docente ed agli alunni, sul corretto e migliore utilizzo consapevole degli strumenti informatici, intesi nel senso globale di servizi e dispositivi, con l'obiettivo di perseguire le finalità non solo giuridiche ma anche educative espresse dal presente Regolamento.

L'Istituto sviluppa l'uso di internet e dei servizi di posta elettronica gestiti dalla rete informatica istituzionale quali strumenti di semplificazione dell'attività amministrativa rivolta agli utenti e per l'ordinaria comunicazione interna ed esterna, nell'ottica di una sempre maggiore dematerializzazione dei documenti cartacei, in conformità alle norme previste dal Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82), alle direttive impartite in materia dal Ministero per la Pubblica Amministrazione e l'Innovazione, nonché dal Garante per la Protezione dei Dati Personali ed ai sensi dell'art. 34, secondo comma, del D.Lgs. 82/2005 e del Regolamento Europeo 679/2016 in materia di protezione dei dati personali (GDPR).

CAPO I MODALITA' DI ACCESSO ED USO DELLA RETE AMMINISTRATIVA

Articolo 1 (Rete Amministrativa e relativi strumenti)

Tutto il personale appartenente alla rete amministrativa è soggetto al Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196 e sue mm.ii.); pertanto per accedere ai personal computer in dotazione è obbligatorio l'utilizzo di un codice di accesso costituito da "nome utente" e "password".

I codici di accesso devono essere custoditi con la massima cura. Nel caso in cui il dipendente non faccia più parte del personale dell'Istituto tali codici saranno annullati.

Tutti i dati lavorati dal personale sono di proprietà dell'Istituto e sono quindi assolutamente vietati la copia e l'esportazione degli stessi su qualsiasi altro supporto o dispositivo, se non preventivamente autorizzata dal Dirigente Scolastico o dal DSGA.
I personal computer della rete amministrativa vengono forniti con tutti i software necessari per l'espletamento delle funzioni assegnate ad ogni utente.
È assolutamente vietato installare o utilizzare software non licenziati o comunque non autorizzati (anche se si tratta di software libero o open source).
È altresì assolutamente vietato salvare dati personali nei pc in dotazione e nei server dell'Istituto.

Articolo 2 (Utilizzo personal computer)

Il personal computer, affidato al personale amministrativo e/o non docente per lo svolgimento dei propri compiti lavorativi, è uno strumento di lavoro ed in quanto tale deve essere utilizzato e custodito da ogni assegnatario con la massima cura e consapevolezza.
Per qualsiasi malfunzionamento o danneggiamento riscontrato, l'utente dovrà informare tempestivamente il Dirigente Scolastico ed il personale tecnico abilitato per i successivi adempimenti di competenza atti a ripristinare nel più breve tempo possibile la funzionalità dello strumento informatico.
Il pc in dotazione deve essere spento ogni giorno da parte dell'utente prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio ovvero per inutilizzo, onde evitare l'indebito utilizzo da parte di terzi non autorizzati.

Art. 3 (Consultazione della posta elettronica e uso di Internet)

La posta elettronica istituzionale, ancorché riferita ad una persona fisica, è uno strumento di lavoro e come tale può essere utilizzata esclusivamente per scopi professionali e lavorativi. È pertanto vietato il suo utilizzo per ogni altro motivo. Tale casella è e resta di proprietà dell'Istituto.
Ogni ufficio ed ogni componente del personale amministrativo, tecnico ed ausiliario abilitato ad una casella di posta elettronica istituzionale è tenuto a consultarla e possibilmente svuotarla quotidianamente, o comunque ogni volta sia necessario, e procedere all'inoltro degli atti secondo le ordinarie modalità operative stabilite nei vari uffici.
La navigazione Internet è possibile da qualunque personal computer abilitato della rete amministrativa. L'utilizzo di Internet è concesso esclusivamente per scopi lavorativi istituzionali.
È previsto un sistema automatico (proxy) di blocco di eventuali siti internet non strettamente attinenti con i compiti e le funzionalità amministrative e/o didattiche.

Art. 4 (Posta elettronica personale)

L'uso di caselle di posta elettronica personali (non riferite a quella istituzionale) è consentito esclusivamente con sistemi web-mail per assolvere ad incombenze amministrative e burocratiche (solo per esempio, per effettuare adempimenti on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e/o assicurativi), ed, in ogni caso, deve essere effettuato al di fuori dell'orario di lavoro e per un uso temporale moderato.

CAPO II MODALITA' DI ACCESSO ED USO DELLA RETE DIDATTICA

Articolo 5 (Rete didattica e relativi strumenti)

L'accesso ai personal computer della rete didattica è libero e privo di codici di accesso personali.

Ogni responsabile di laboratorio decide le modalità di accesso degli allievi e del personale docente e non docente del laboratorio a lui assegnato. Dovrà essere comunque riservato un accesso al personale tecnico dell'Istituto al fine di permettere, in qualunque momento, gli interventi tecnici che si rendessero necessari per il corretto funzionamento dei dispositivi informatici.
I personal computer della rete didattica vengono forniti di tutti i software necessari per l'espletamento dell'attività didattica.
Alla fine di ogni anno scolastico i responsabili di laboratorio dovranno stilare una lista di programmi e funzionalità necessari alla didattica dell'a.s. successivo, da inoltrare tempestivamente al personale tecnico incaricato dall'Istituto per gli adempimenti di competenza.
Non è consentita l'installazione od utilizzo di software *non licenziati* o comunque non preventivamente autorizzati, anche in caso di programmi c.d. 'liberi' o 'open source'. È fatto divieto di salvare dati personali di qualsiasi genere nei personal computer della rete didattica e nei relativi server dell'Istituto.

Articolo 6 (Consultazione della posta elettronica e uso di Internet)

I docenti abilitati ad una casella di posta elettronica istituzionale devono consultarla quotidianamente, e comunque ogni volta sia necessario, e procedere all'inoltro degli atti secondo le ordinarie modalità operative stabilite nei vari uffici.
La navigazione Internet, concessa esclusivamente per scopi didattici istituzionali, è possibile dal qualunque personal computer abilitato della rete didattica, previo inserimento di codici di accesso personali. I codici di accesso sono generati dallo Staff Informatico e devono essere custoditi da parte degli assegnatari con la massima cura. La "password" provvisoria assegnata per il primo accesso dovrà essere immediatamente sostituita dall'utente con una personale. Nel caso in cui il docente non presti più servizio presso l'Istituto, tali codici saranno cancellati.
È previsto un sistema automatico (proxy) di blocco di eventuali siti internet non strettamente attinenti con i compiti e le funzionalità amministrative e/o didattiche.

Articolo 7 (Posta elettronica personale)

L'uso di caselle di posta elettronica personali (non riferite a quella fornita dall'Istituto) è consentito esclusivamente con sistemi web-mail per assolvere ad incombenze amministrativo-burocratiche (solo per esempio, per effettuare adempimenti on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e/o assicurativi), ed, in ogni caso, deve essere effettuato al di fuori dell'orario di lavoro e per un uso temporale moderato. E' consentito altresì l'uso delle caselle di posta elettronica personali da parte del personale docente per lo scambio di avvisi ed informazioni necessari per lo svolgimento delle varie attività didattiche.

Articolo 8 (Utilizzo dei mezzi informatici)

I personal computer, i notebook, i tablet, le LIM, i televisori ed i proiettori, nonché i relativi accessori, presenti nelle aule e laboratori dell'Istituto sono una risorsa preziosa per la didattica e l'insegnamento, e richiedono un utilizzo corretto e consapevole da parte di tutto il personale, docente, non docente ed alunni.
Non è consentita la movimentazione e/o la preparazione, per le varie attività didattiche, di detti strumenti da parte degli allievi se non preventivamente autorizzata dal docente responsabile. Durante l'intervallo e/o i cambi dell'ora, è compito del docente vigilare sulla permanenza di ogni singolo strumento informatico in condizioni di sicurezza e di efficiente funzionamento. A tal proposito all'interno dei laboratori deve essere garantita la presenza di almeno una persona (docente, itp o assistente tecnico); nel caso in cui cio' non sia possibile, il laboratorio deve essere chiuso.
Qualora sorgessero problemi di malfunzionamento e/o danneggiamento, il docente o il coordinatore di classe deve segnalare il fatto al personale tecnico dell'Istituto, informando nei casi più gravi il Dirigente Scolastico.

Articolo 9 (Utilizzo dei software)

Il sistema operativo, tutti i moduli e programmi software messi a disposizione dell'Istituto non possono essere utilizzati per attività personali o a fini di lucro.
È assolutamente vietato copiare e/o utilizzare dei programmi di proprietà personale all'interno dei personal computer dell'Istituto. In presenza di particolari esigenze didattiche, sarà il docente di riferimento a segnalare agli incaricati tecnici la necessità di installazione di nuovo software.
I software a disposizione sulla rete didattica non possono essere copiati e/o distribuiti su dispositivi esterni, salvo per quanto esplicitamente consentito dall'Istituto sulle aree di pubblico dominio, nel rispetto degli accordi specificamente assunti.
Non è ammesso l'utilizzo di programmi e software per attività di tipo ricreativo e ludico, e comunque non strettamente legati alla didattica od alla ricerca.

È fatto divieto di utilizzare o di possedere programmi c.d. "cavalli di troia", ed in generale programmi e/o software di qualsiasi genere atti a violare la sicurezza dei sistemi locali o remoti.
Poichè tutti gli strumenti informatici presenti in istituto, fissi o mobili, di proprietà della scuola o dei singoli, sono utilizzati per scopi didattici, è fatto divieto di installare giochi. Solo in casi eccezionali, con autorizzazione del docente, gli studenti potranno accedere ad applicazioni ricreative con valenza didattica (es. gioco degli scacchi).

Articolo 10 (Cessione utilizzo del laboratorio a terze parti)

Nel caso in cui venga autorizzato l'uso dei laboratori da parte di soggetti od enti esterni per corsi di aggiornamento, post-diploma, concorsi e/o attività extrascolastiche in genere, il
Dirigente Scolastico coordinerà l'attività prevista con il consegnatario dei beni, il responsabile della gestione locali e l'amministratore di rete. I responsabili esterni delle attività extrascolastiche dovranno prendere contatto con il responsabile dei laboratori al fine di prendere visione della dotazione dei laboratori stessi e del relativo regolamento di gestione ed utilizzo.
Nella concessione dei laboratori per gli scopi di cui al comma precedente, il Dirigente Scolastico dovrà comunque tenere conto della disponibilità dei laboratori stessi con priorità alle necessità didattiche evidenziate dai docenti dell'Istituto.

Articolo 11 (Prestiti di materiale di laboratorio)

L'hardware ed il software presenti nei laboratori possono essere prestati a studenti e/o a personale dell'Istituto previa richiesta motivata ed autorizzata dal Dirigente Scolastico. Il prestito va annotato nel registro di presenze del laboratorio, a cura del responsabile del laboratorio medesimo.

CAPO III PERSONALE TECNICO E SICUREZZA INFORMATICA

Articolo 12 (Personale tecnico)

Il personale dipendente tecnico dell'Istituto è il solo autorizzato a compiere interventi nel sistema informatico dell'Istituto, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici/manutentivi (ad esempio, aggiornamenti, sostituzioni e implementazioni di programmi e software, manutenzioni hardware, etc..).
Detti interventi, in considerazione dei divieti presenti nel presente Regolamento, con particolare riferimento a quelli di cui al successivo Capo IV, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascun utente, compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata o di impedimento anche dell'utente.

Articolo 13 (Interventi del personale tecnico)

Il personale tecnico incaricato del servizio di assistenza tecnica ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC esclusivamente al fine di garantire l'assistenza tecnica necessaria e la normale attività operativa, amministrativa e didattica, nonché la massima sicurezza contro virus, spyware, malware e simili. L'intervento viene effettuato su richiesta dell'utente o, in caso di oggettiva od urgente necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Articolo 14 (Sicurezza Informatica - Antivirus)

Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato. Ogni utente deve comunque porre in essere comportamenti tali da ridurre al massimo il rischio di attacco al sistema informatico dell'Istituto mediante virus informatici o ogni altro software aggressivo.

Nel caso il software antivirus dovesse rilevare la presenza di virus pericolosi, l'utente dovrà immediatamente sospendere ogni elaborazione in corso disconnettendo il computer dalla rete, nonché segnalare prontamente l'accaduto al personale tecnico incaricato ed al Dirigente Scolastico.

Art. 15 (Dispositivi esterni)

Ogni dispositivo magnetico, pen drive, chiavette usb e simili di provenienza esterna all'Istituto dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga segnalata la presenza di un virus, dovrà essere prontamente rimosso dal pc e consegnato al personale tecnico incaricato per le opportune verifiche.

CAPO IV DIVIETI E SANZIONI

Art. 16 (Operazioni non autorizzate)

È vietata a studenti, docenti ed al personale tecnico e amministrativo l'installazione di programmi non autorizzati sulle postazioni informatiche dell'Istituto. Qualora fosse necessario, solo ed esclusivamente per fini didattici o amministrativi, installare software non ancora in dotazione all'Istituto, il diretto interessato deve produrre apposita richiesta al
Dirigente Scolastico specificando tipo di programma, utilizzo, eventuale costo ed attività interessate. Solo successivamente al visto di approvazione rilasciato da parte di una commissione costituita dal Dirigente Scolastico, D.S.G.A. ed Ufficio tecnico, si potrà procedere all'eventuale acquisto e/o installazione del software richiesto.

È vietata la pubblicazione nel sito dell'Istituto di qualsiasi documento, sia esso didattico o amministrativo, prima che la stessa sia stata autorizzata dal Dirigente Scolastico, che avrà provveduto a vistare il materiale.

È vietata l'installazione di propri programmi. È altresì vietata l'installazione di propri dispositivi senza l'autorizzazione del Dirigente Scolastico o senza la preventiva scansione con un valido antivirus dell'Istituto.
È vietato modificare i programmi installati nei pc o alterarne le configurazioni agendo su software o hardware.

È vietato accedere ai servizi utilizzando l'account di un altro utente, fatta eccezione per l'accesso, da parte di altro personale addetto ed appositamente autorizzato per motivi d'ufficio o funzionali, a siti istituzionali consultabili esclusivamente mediante l'utilizzo di un'unica credenziale assegnata d'ufficio al D.S. o ad altra persona allo scopo individuata.

Articolo 17 (Sanzioni)

È fatto obbligo a tutti gli utenti (personale docente, non docente, amministrativo, tecnico ed alunni) di osservare le disposizioni di cui al presente Regolamento. Il mancato rispetto o la violazione delle norme in esso contenute è perseguibile con provvedimenti disciplinari e risarcitori previsti dalle norme, contratti e regolamenti vigenti, nonché con tutte le azioni civili e penali previste.

CAPO V NORME DI COMPORTAMENTO E DI LEGGE

Articolo 18 (Relazioni tra cittadini digitali)

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

Articolo 19 (Decalogo di comportamento dell'utente)

Ai sensi dell'articolo precedente, è buona norma osservare, da parte dell'utente del *web*, le seguenti regole di comportamento:

- Occorre contribuire a rendere il *web* un luogo sicuro; pertanto ogni volta che un utente commette un abuso o un errore pubblicando materiale illecito, non idoneo od offensivo, occorre contattarlo e fornire le spiegazioni relative alle regole da seguire, diffondendo in tal modo i principi della sicurezza e correttezza.
- Ogni abuso subìto o rilevato nella navigazione deve essere segnalato tramite gli strumenti legali offerti dal servizio per ottenere la rimozione del contenuto. Prima di trasformare un incidente o una bravata in una denuncia alle Autorità competenti, vale la pena di segnalare il fatto ai gestori del relativo sito per non incorrere in conseguenze penali e giudiziarie.
- Se si condividono informazioni personali, prima della pubblicazione occorre scegliere con cura cosa rendere pubblico e cosa mantenere privato; scegliere con attenzione le amicizie con cui accrescere la propria rete e proteggere la propria identità digitale con password.
- Se si condividono elementi multimediali od informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare qualsiasi pubblicazione. Non si devono pubblicare video girati di nascosto all'interessato/i e dove sono presenti persone riprese senza il loro consenso.
- Evitare di scambiare file con utenti di cui non ci si può fidare; in ogni caso, anche quando si conosce l'interlocutore, è bene verificare sempre l'origine del file ed effettuare un controllo con un antivirus aggiornato.
- Se durante una conversazione on-line l'interlocutore diviene volgare, offensivo o minaccioso, si deve abbandonare la conversazione.
- Nell'uso di sistemi di file-sharing P2P (peer-to-peer), evitare di scaricare dei file che possono essere considerati illegali e/o protetti dal diritto d'autore; non aprire mai dei file sospetti (la maggior parte dei programmi P2P contiene spyware e malware). Per motivi di sicurezza la scuola vieta l'utilizzo di questi sistemi.
- I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica; quindi, quando si invia un messaggio a più destinatari che non si conoscono tra loro, è necessario evitare che i destinatari possano vedere e conoscere i propri indirizzi di posta elettronica.
- Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo è necessario essere sicuri di averne il diritto d'uso e di non utilizzare file coperti da copyright senza la necessaria autorizzazione.

- I contenuti pubblicati sulle applicazioni web dei Social Network hanno diversi livelli di visibilità (es. singoli utenti o tutti gli utenti della rete) che devono essere tenuti a mente dando a ciascun contributo i corretti livelli di privacy.
- Quando si contribuisce a pubblicare materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto, evitando di pubblicare materiale inadeguato: ci sono luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori.
- La reputazione digitale si diffonde velocemente; pertanto, non si devono diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito.
- È possibile la pubblicazione di foto di alunni purché queste riguardino momenti positivi di vita scolastica, dato che con l'informativa sulla privacy, fornita al momento dell'iscrizione, le famiglie sono state informate dell'evenienza in questione.

Articolo 20 (Utilizzo dispositivi e reti mobili personali)

Ai sensi del D.P.R. n. 249/1998 ed alla luce della circolare del Ministro della Pubblica Istruzione del 15 marzo 2007, la telefonia mobile, ed i relativi dispositivi, di esclusiva proprietà degli studenti è consentita solo al di fuori dei locali (e pertinenze) dell'Istituto, nel rispetto dei principi educativi e di correttezza previsti dallo Statuto delle studentesse e degli studenti.
Durante l'orario scolastico agli studenti non è permesso l'utilizzo della telefonia mobile, in nessuna funzione, nonché l'uso per scopo personale di tutti gli altri strumenti informatici di esclusiva proprietà dello studente. Rientra nell'uso improprio degli strumenti informatici personali lo scaricamento e/o l'utilizzo di giochi (art.9).
Resta fermo che, anche durante lo svolgimento delle attività didattiche, eventuali esigenze di comunicazione tra gli studenti e le rispettive famiglie, dettate da ragioni di particolare urgenza o gravità, potranno sempre essere soddisfatte, previa autorizzazione del docente. L'Istituto, in ogni caso, garantisce sempre la possibilità di una comunicazione reciproca tra le famiglie ed i propri figli studenti, per gravi ed urgenti motivi, mediante gli uffici di presidenza e di segreteria amministrativa.
Il divieto di utilizzare telefoni o dispositivi informatici privati durante lo svolgimento di attività di insegnamento/apprendimento, opera anche nei confronti del personale docente e non docente, in considerazione dei doveri derivanti dal CCNL vigente e dalla necessità di assicurare all'interno dell'Istituto le migliori condizioni per uno svolgimento sereno ed efficace delle attività didattiche, salvo che detti dispositivi o telefoni personali non debbano essere utilizzati dai docenti per particolari e/o contingenti scopi didattici.
L'eventuale utilizzo di strumenti informatici di proprietà esclusiva dello studente durante una specifica attività didattica deve essere autorizzato preventivamente dal Dirigente Scolastico a seguito di richiesta del docente, le cui specifiche modalità di utilizzo concordate saranno sotto la responsabilità e la vigilanza costante del docente medesimo.

CAPO VI REATI E VIOLAZIONI DI LEGGE

Articolo 21 (Reati Informatici)

La legge 547/1993 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi degli interessi non solo di singoli privati cittadini, ma anche di persone giuridiche, in particolare di imprese ed enti pubblici:

- ***Accesso abusivo ad un sistema informatico e telematico***: per commettere il reato è sufficiente il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC ad 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 sui quali non siamo autorizzati (615 ter cp).

- ***Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico***: l'art. 615 quinquies punisce "chiunque diffonde, comunica e consegua 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 e 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 un qualsiasi programma di messenger o posta elettronica, spiegare ad altre persone come si può fare per sproteggere un computer, un software o una console o un dispositivo, 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. È 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 involontariamente, i codici di accesso alla posta elettronica, ai messenger o ai profili di amici e compagni.

- ***Frode informatica***: questo reato discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danni" (art. 640 ter cp). Il profitto può anche non avere carattere economico, potendo consistere 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.

Articolo 22 (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 delittuoso:

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

- ***Diffamazione***: si verifica quando si offende la reputazione di qualcun altro, o quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona (art. 595 cp). Costituisce un'aggravante il 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 ed 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). Il reato di molestie e disturbo alle persone, disciplinato dall'art. 660 cp, 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 numero di cellulare di una persona on-line, accompagnato da informazioni non veritiere o ingiuriose. Ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite.

- ***Violazione dei diritti d'autore***: la legge n. 633 del 22 aprile 1941 e ss.mm.
sottolinea all'art. 1 che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali ovvero pone in commercio, detiene per la vendita o introduce a fini di lucro le copie, viola i diritti d'autore. Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti. In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato è sufficiente pubblicare su YouTube (ad esempio) 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 (ad es., in 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.