

# Diritto e informatica

## Prerequisiti specifici

### CONOSCENZE

- ◆ Principali aspetti legati alla sicurezza di un sistema informatico

### ABILITÀ

- ◆ Comprendere la normativa sul diritto d'autore e sul diritto

alla privacy

- ◆ Riconoscere i crimini informatici ed essere consapevoli delle conseguenze giuridiche
- ◆ Comprendere gli aspetti giuridici e fiscali del commercio elettronico

## Obiettivi specifici

### CONOSCENZE

- ◆ Conoscere la normativa sul diritto d'autore
- ◆ Conoscere la normativa sul diritto alla privacy
- ◆ Conoscere la normativa sul commercio elettronico

- ◆ Conoscere la normativa sui reati informatici

### ABILITÀ

- ◆ Saper individuare i reati informatici
- ◆ Saper classificare il software in base al tipo di licenza d'uso

## 1 Perché il diritto in un libro di informatica?

Un mondo con coinvolgimenti sociali ed economici come quello informatico non può che ricadere necessariamente sotto la tutela del diritto. È molto sentita, infatti, l'esigenza di un adeguamento della normativa, al fine di scoraggiare e prevenire alcuni tipi di crimine e tutelare il lavoro degli sviluppatori. In questa unità non possiamo certamente fare una panoramica completa della legislazione in materia, ma daremo comunque alcune indicazioni e riferimenti normativi su:

- la tutela giuridica del software: il **diritto d'autore**;
- alcuni aspetti della **criminalità informatica**;
- la tutela della **privacy**;
- gli aspetti contrattuali nel **commercio elettronico**.

## 2 La tutela giuridica del software

Affrontiamo adesso vari aspetti relativi alla tutela giuridica del software.

### 2.1 Diritto d'autore e normativa

I programmi per elaboratore sono tutelati **civilmente e penalmente** dalla **normativa sul diritto d'autore**, in quanto opere dell'ingegno, che si esprimono in linguaggio tecnico-convenzionale, concettualmente parificabile all'alfabeto o alle sette note. Sentenza della Corte di Cassazione del 24/11/86. Il requisito della creatività è dato dalla novità e dall'originalità dello sforzo intellettuale.

“ Il **diritto d'autore** o **copyright** può essere definito come il diritto riconosciuto all'autore di un'opera dell'ingegno di carattere creativo, a discapito della libera utilizzazione da parte della collettività. ”

Nell'ordinamento italiano, la normativa a tutela del software è stata codificata con l'apposita **legge n. 518 del 1992**, che ha esteso al software la tutela già prevista per le altre opere dell'ingegno con la **legge n. 633 del 1941** sul diritto d'autore. Quest'ultima legge era già stata dichiarata applicabile al software da numerose sentenze giurisprudenziali (una delle prime risale alla pretura di Pisa nel 1984).

L'**algoritmo** finalizzato alla soluzione del problema è **opera dell'ingegno ed è brevettabile**. Ma vediamo cronologicamente quali sono stati i passaggi legislativi:

1. con delibera del 14 maggio 1991 il Consiglio della Comunità Europea approva la **Direttiva 91/250** relativa alla tutela giuridica dei programmi per elaboratore;
2. con l'articolo 7 della **legge n. 489 del 19 dicembre 1992** si mette in attuazione la precedente direttiva comunitaria;
3. con il **Decreto legge n. 518 del 29 dicembre 1992** si è recepita la direttiva comunitaria e si è modificata la **legge n. 633 del 22 marzo 1941** sul diritto d'autore, inserendo anche la tutela giuridica dei programmi per elaboratore;
4. con il **Decreto legislativo 169 del 1999** la legge sul diritto d'autore è stata estesa anche alle banche dati;
5. con la **legge n. 248 del 2000** è stato inasprito il regime sanzionatorio per la duplicazione e la diffusione di software pirata.
6. Con il **decreto URBANI**, decreto legge del 12/04/2004, viene considerato reato la diffusione al pubblico per via telematica anche mediante programmi di **file sharing** (condivisione di file tra utenti), di un'opera cinematografica protetta da diritto d'autore. La legge prevede una sanzione pecuniaria amministrativa. Anche per la sola fruizione di un'opera cinematografica on-line.

Con quest'ultima legge è stata prevista, per la prima volta nell'ordinamento italiano, la possibilità di perseguire penalmente chiunque acquisti o detenga software pirata anche per uso strettamente personale (costituisce reato anche la duplicazione di un videogioco originale da un amico). L'autore può anche registrare a pagamento un software presso la **SIAE (Società Italiana Autori ed Editori)**, istituto che gestisce il **pubblico registro speciale** per i programmi per elaboratore (articolo 103 comma 4 della legge sul diritto d'autore). Un requisito indispensabile è che il software presenti carattere creativo, cioè originalità rispetto ai programmi preesistenti. Può essere registrato sia software già messo in commercio o già distribuito sia software inedito. Il software inedito viene depositato su supporto inserito in busta chiusa e sigillata dalla SIAE.

Tale registrazione non è obbligatoria come per le opere letterarie o le altre opere dell'ingegno, ma offre all'autore una maggiore tutela sia dal punto di vista penale (perché sono previste sanzioni più severe per la violazione del diritto d'autore del software registrato), sia dal punto di vista civilistico (perché costituisce *prova della paternità* della creazione del software e garantisce *data certa della creazione*).

Comunque la legge tutela la sola **forma espressiva** del programma, non le idee o i principi che ne sono alla base. Ciò che non si può imitare o copiare è la forma finale, il *confezionamento* (da distinguere dalla confezione).

## ESEMPIO

Non è tutelata l'idea di realizzare un programma di elaborazione testi, ma non si può copiare il prodotto finito (quello in commercio), che è quello tutelato.

In alcuni Stati le cose possono essere radicalmente diverse. Ad esempio, nella normativa statunitense la tutela del software ricade sia nell'ambito della tutela d'autore sia in quello dei brevetti e delle invenzioni industriali (come in Giappone).

A livello internazionale, infatti, la normativa è abbastanza generica e prevede “*le forme di tutela del software che meglio si armonizzano con l’ordinamento interno di ogni Stato*”. Ciascuno Stato ha quindi recepito il principio generale della normativa internazionale armonizzando la tutela del software col proprio sistema legislativo.



Nell’ambito nella Comunità Europea si è discusso se introdurre o meno una tutela brevettuale del software o di alcune sue particolari tipologie. La tutela brevettuale è stata osteggiata dai fautori del software open source, i quali ritengono che la brevettabilità delle idee che sono alla base anche solo di una parte del software impedirebbe a qualsiasi altro programmatore di realizzare un programma basato su idee analoghe. Il brevetto per un algoritmo che calcola la somma degli elementi di un vettore, impedirebbe di

realizzare ogni altro algoritmo con la stessa finalità. I piccoli programmatori temono che le grandi compagnie possano brevettare tutto il “brevettabile” e poi chiedere un risarcimento alle piccole aziende che anche senza saperlo possano avere adottato nei propri programmi idee tutelate da brevetto. Le grandi software house sostengono, invece, che la tutela brevettuale possa meglio tutelare gli investimenti nella ricerca e favorire lo sviluppo del software. L’ultima proposta di introdurre una tutela brevettuale, pochi mesi fa è stata bocciata.

## 2.2 La decompilazione

La **decompilazione**, ovvero il risalire dal codice oggetto al codice sorgente, dopo aspra discussione in materia, è stata **vietata** in generale con l’articolo 64 bis del **Decreto legislativo 518/92**, sebbene con alcune eccezioni.

I casi in cui la decompilazione è **permessa** sono quelli in cui essa sia indispensabile per ottenere l’**interoperabilità con altri programmi**, purché:

- si abbia la *licenza d’uso* del software;
- le informazioni necessarie per ottenere l’interoperabilità non siano *immediatamente accessibili*;
- si *decompili* solo la parte necessaria a ottenere l’interoperabilità.

Ad esempio, il grande successo di Windows è dovuto al fatto che la Microsoft ha permesso l’interoperabilità con qualsiasi programma sviluppato da altre case produttrici, dettando le modalità tecniche con cui tale interoperabilità poteva avvenire.

L’articolo 64 *ter* Decreto legge 518 recita che la **decompilazione** è sempre possibile nei casi in cui occorra:

*“osservare, studiare e sottoporre a prove il funzionamento del programma, allo scopo di determinare idee e principi su cui è basato ogni elemento del programma stesso”.*

## 2.3 Le sanzioni nella legge penale italiana

L’obiettivo della legge era quello di **limitare** al massimo un illecito uso commerciale dei programmi per computer. In linea con quanto sanzionato in materia di violazione del diritto d’autore per le opere letterarie e/o artistiche previsto nella *Legge 633/41*, sono state previste pene detentive varianti da tre mesi a tre anni e pene pecuniarie anche considerevoli, in particolare per i **reati di**:

- *duplicazione* di software a fini di profitto (senza averne titolo);
- *importazione, distribuzione, vendita, detenzione* di software pirata;
- concessione in *locazione* di programmi;
- *manomissione* di dispositivi di protezione;
- scambio attraverso programmi di file sharing (peer to peer) di opere cinematografiche.

Appare evidente come l’elemento lucrativo (incremento patrimoniale o di profitto che può consistere anche in un risparmio di spesa) caratterizzi ogni tipo di reato. Ricordiamo che

l'unica copia che può essere fatta dal detentore di software originale è una *copia per fini di sicurezza (copia di back-up)*.

## 2.4 Le licenze d'uso

È l'autore che decide cosa permettere a chi acquista il suo software. Occorre a questo punto distinguere, nell'ambito del **diritto d'autore**, due diritti fondamentali:

- diritto **morale** d'autore, che a sua volta si divide in:
  - diritto alla **paternità** dell'opera;
  - diritto all'**integrità** dell'opera (cioè il diritto di opporsi a ogni mutamento, modifica, deformazione che possano recare pregiudizio all'onore e alla reputazione dell'autore);
  - il diritto di **pubblicazione** (cioè il diritto che sia divulgato o rimanga inedito);
  - il diritto di **pentimento** (cioè il diritto di ritirare l'opera in commercio per gravi ragioni morali: tempo addietro successe che l'autore di un famoso algoritmo di crittografia si pentì di aver messo in commercio un programma che veniva abilmente utilizzato dalla malavita organizzata);
- diritto di **utilizzazione economica**, che si divide in:
  - diritto di **riproduzione** totale o parziale;
  - diritto di **traduzione, adattamento e ogni altra modifica** (non pregiudizievole dell'onore e della reputazione dell'autore);
  - diritto di **distribuzione al pubblico** (compresa la locazione).

I **diritti morali** sono strettamente connessi alla personalità dell'autore, mentre quelli di **utilizzazione economica** consentono di sfruttare commercialmente il software.

### ESEMPIO

Se un utente acquista Netscape Navigator (inizialmente veniva venduto), acquista la licenza d'uso per un utilizzo personale del software così come è stato prodotto. Quando la Sun Microsystems ha acquistato invece il diritto di utilizzazione economica di Netscape Navigator ha potuto disporre pienamente di tale software, potendolo modificare, distribuire gratuitamente (come ha poi fatto) ecc.

Quando noi acquistiamo software, in realtà stiamo acquistando la **licenza d'uso**, cioè il diritto a "utilizzare quel software" in via esclusivamente personale.

La licenza d'uso coincide con il **diritto d'uso** e non con il diritto di **utilizzazione economica** di quel software.

Finora abbiamo parlato della generica tutela del software che la legge offre agli sviluppatori; non tutti gli autori, però, desiderano tutelare allo stesso modo le proprie creazioni. Da ciò derivano diverse tipologie di tutela corrispondenti ad altrettante licenze.

## 2.5 Una classificazione del software

Prima di addentrarci nella classificazione del software, occorre evidenziare, schematizzando, le due opposte filosofie presenti attualmente nel mondo dell'informatica:

- 1) *"il software è un prodotto industriale"*:  
 "il software è un **prodotto industriale** il cui codice sorgente è **segreto industriale**; chi copia, diffonde, modifica il software è un **criminale informatico** e va perseguito".  
 Sono esempi di questa filosofia tutte le licenze d'uso di software proprietari;
- 2) *"il software è un patrimonio dell'umanità"*:  
 "il software è un **patrimonio inalienabile dell'umanità** (di cui cioè non ci si può appropriare). Chi copia, diffonde e modifica il software accresce tale patrimonio ed è quindi un **benefattore**".  
 Sono esempi le licenze **GPL** di alcuni software liberi (che vedremo in seguito).

Ovviamente tra queste due filosofie opposte si collocano tutte le altre che andiamo a scoprire implicitamente classificando il software.

Vediamo in dettaglio le seguenti categorie di software, tralasciando sfumature che in questo contesto non sono importanti:

- software *libero* (*open-source*):
  - software libero *con permesso d'autore* (copyleft);
  - software libero *senza permesso d'autore o di pubblico dominio*;
- software *semilibero*;
- software *proprietario*;
- *freeware*;
- *shareware*;
- software *commerciale*.

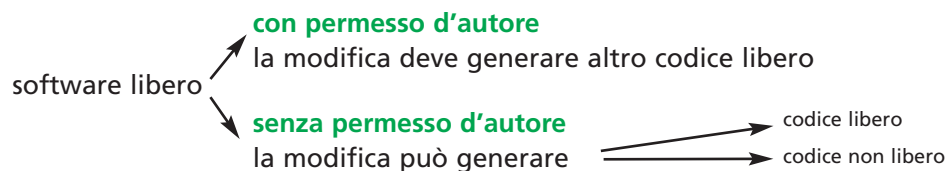
### 2.5.1 Software libero o open source

In modo semplificato possiamo dire che il **software libero** o **open source** è un software distribuito insieme al suo codice sorgente. Chiunque può avere il permesso di uso, copia e distribuzione (in forma modificata o meno).

Il termine **software libero** si riferisce alla libertà e non al prezzo. Molte case costruttrici talvolta usano il termine **free software** per riferirsi al prezzo (attenzione: in inglese *free* vuol dire sia *libero* che *gratuito*). Alcune volte ciò significa che si può ottenere una copia del binario (del file oggetto) senza pagarla, altre volte significa che una copia è inclusa nel computer che si sta acquistando, ma questo non ha nulla a che vedere con il concetto di software libero.

“ Possedere un **software libero** vuol dire avere a disposizione il suo codice sorgente e l'eventuale possibilità di distribuzione anche a fini di lucro del software originale o modificato. ”

Il software libero viene **classificato** in base al tipo di software che possiamo ottenere modificandolo:



- **Software libero con permesso d'autore (copyleft)**

Il software **con permesso d'autore** è software libero le cui condizioni di distribuzione non permettono a chi lo ridistribuisce di porre alcuna restrizione ulteriore all'atto di ridistribuire o modificare il software. Questo significa che ogni copia del software, anche se modificata, deve essere comunque una copia di software libero. Notiamo che il termine "permesso d'autore" contiene un gioco di parole. Infatti: **copyright** (*diritto d'autore*) è formato da **copy** (che significa *copia*) e **right** (che significa *diritto*, ma anche *destra*). L'opposto è **copyleft**, dove **left** significa *lasciato*, ma anche *sinistra*.

In sostanza:

“ il software con **permesso d'autore** è un software che comprende i sorgenti (è infatti software libero), ma con una restrizione che obbliga chi lo ridistribuisce (anche dopo aver apportato le proprie modifiche) a lasciarlo libero. ”

La **licenza GPL** (*General Public License*), assai diffusa nel mondo dell'informatica, è un caso particolare di software con permesso d'autore.

- **Software libero senza permesso d'autore o software di pubblico dominio (public domain)**

Il software **senza permesso d'autore o di pubblico dominio** è software libero con restrizioni sulla distribuzione del risultato della sua modifica. Se un programma è libero, ma è senza permesso d'autore, alcune copie o versioni modificate potrebbero non essere affatto libere. Un'azienda di software potrebbe infatti compilare il programma e distribuire il file eseguibile come software proprietario.

Un esempio di tale tipo di software è l'*X11 Windows System*. L'*X Consortium* realizzò *X11* con termini di distribuzione che lo rendevano software libero senza permesso d'autore. Volendo, si può ottenere una copia che ha quelle condizioni di distribuzione ed è software libero. Tuttavia, esistono anche versioni non libere, e ci sono *Workstation* e schede grafiche per le quali tali versioni non libere sono le uniche che funzionano. Quindi, chi intende usare quell'hardware deve acquistare il software non libero.

Il software di pubblico dominio è software **privo di copyright**. Talvolta si usa il termine "dominio pubblico" in un'accezione vaga per intendere "libero" o "disponibile gratuitamente".

Tuttavia "dominio pubblico" è un termine legale che significa precisamente "**senza copyright**". Per chiarezza, conviene utilizzare il termine "di dominio pubblico" solo con questo significato.

### 2.5.2 Software semilibero

Il **software semilibero** è software non libero, quindi non è rilasciato con i sorgenti, ma è distribuito con il permesso per i privati di essere usato, copiato, distribuito e modificato (incluse le versioni distribuite con modifiche) **senza scopo di lucro**.

PGP (il famoso programma di crittografia a chiave pubblica) è un esempio di programma semilibero.

Il software semilibero non può essere usato in un sistema operativo libero.

### 2.5.3 Software proprietario

Il **software proprietario** è software normalmente in commercio, in genere per aziende e professionisti. A volte non è rilasciato con i sorgenti, la sua copia e distribuzione sono proibite o a pagamento.

### 2.5.4 Freeware

Il **freeware** non ha una definizione comunemente accettata, ma è utilizzato per pacchetti software che possono essere ridistribuiti, ma non modificati, e il cui *codice sorgente non è disponibile*.

Questi pacchetti *non sono software libero*, il loro uso e distribuzione con o senza scopo di lucro è comunque gratuito.

### 2.5.5 Shareware

Lo **shareware** è software concesso in utilizzo *per un limitato periodo di tempo* decorso il quale, se l'utente trova il prodotto di proprio gradimento, deve obbligatoriamente acquistare la licenza d'uso.

In qualche caso viene fornita a scopo valutativo una vecchia *release* del programma o una sua versione non completamente funzionante, in altri casi vengono inserite delle routine che rendono impossibile l'uso del software se non viene registrato entro un certo termine. Generalmente gli autori di software *shareware* danno la possibilità a chiunque ne venga in possesso di ridistribuirlo.

Lo **shareware** è software che dà la possibilità di ridistribuire copie, ma impone a chiunque continui a usarne una copia di pagare la licenza d'uso.

Lo shareware non è software libero, non è semilibero e nemmeno gratuito perché:

- per la maggior parte dei software shareware il *codice sorgente* non è disponibile, pertanto non è possibile modificare il programma;
- il software shareware non è distribuito con il permesso di utilizzarlo *senza pagare la licenza d'uso*, neanche se l'utilizzo è senza fini di lucro.

### 2.5.6 Software commerciale

Il software commerciale rappresenta una categoria trasversale a quelle viste precedentemente. Si tratta di software sviluppato da un'azienda allo scopo di guadagno. Quindi il suo uso o la sua distribuzione sono a scopo di lucro. Può essere libero oppure no. Il significato del termine "commerciale" è quindi diverso da quello di "proprietario".

Se è infatti vero che la maggior parte del software commerciale è anche proprietario, esiste sia software commerciale libero sia software non commerciale non libero.

Possiamo riepilogare tale classificazione nel seguente schema:

#### Le licenze del software

	DISPONIBILITÀ SORGENTI	POSSIBILE DISTRIBUZIONE CON LUCRO	POSSIBILE DISTRIBUZIONE SENZA LUCRO	POSSIBILE USO CON LUCRO	POSSIBILE USO SENZA LUCRO	POSSIBILE MODIFICA	COMMERCIALE
Proprietario	NO	NO	NO	NO	NO	NO	SÌ
Shareware	NO	SÌ	SÌ	NO	NO	NO	SÌ
Freeware	NO	SÌ	SÌ	SÌ	SÌ	NO	NO
Semilibero	NO	NO	SÌ	NO	SÌ	SÌ	SÌ/NO
Libero con permesso d'autore	SÌ	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO	SÌ	SÌ/NO
Libero senza permesso d'autore	SÌ	SÌ	SÌ	SÌ	SÌ	SÌ	SÌ/NO

Menzioniamo alla fine anche tutto ciò che è prodotto e visualizzato attraverso l'utilizzo di software come, ad esempio, tutta l'informazione digitale (pagine Web, ipertesti, musica prodotta in digitale, video ecc.) è tutelato dal diritto d'autore, né più né meno come un libro, un CD musicale o un film.

## 3 Criminalità informatica

I cambiamenti radicali nelle comunicazioni interpersonali e il costante incremento dell'utilizzo delle tecnologie informatiche in settori fondamentali della società, quali il lavoro, la pubblica amministrazione, la ricerca scientifica, hanno reso necessaria una modifica (o meglio una costruzione) normativa che tutelasse questo complesso e capillare sistema telematico.

Senza entrare nel labirinto di leggi, decreti, direttive, indichiamo i principali crimini per la prima volta introdotti dalla **legge n. 547 del 23 dicembre 1993**, reati penali comunemente definiti come **computer crime**. Dovendo tutelare il software, occorre precisare la differenza di interpretazione di una norma esistente tra il diritto civile e quello penale. Nel **diritto civile** infatti è applicabile l'**interpretazione in via analogica**. Ciò vuol dire che, per valutare un caso, è possibile far riferimento a un caso simile o analogo e applicare la norma che è stata applicata in tale caso.

Nel **diritto penale** invece l'interpretazione analogica **non è possibile**. Parlando di tutela del software, le considerazioni appena fatte implicano che nel diritto civile, *prima della legge*

518, era comunque possibile utilizzare l'interpretazione per via analogica e quindi si equiparava il software alle opere letterarie. Nel diritto penale ciò non era possibile, quindi vi era una effettiva carenza legislativa (penale) in materia di tutela del software. La legge n. 547 del 1993 è quindi un passaggio importante perché, *per la prima volta*, introduce i reati di tipo penale, che andiamo subito ad analizzare.

### 3.1 Tipologie di reato e sanzioni dei principali crimini informatici

Di seguito vengono elencati alcuni reati contemplati dalla legge 547/93:

- **attentati a impianti di pubblica utilità.** *L'articolo 420* punisce chiunque commetta un fatto volto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità (ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti). La pena è più grave se dal fatto deriva la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione (anche parziale) del funzionamento del sistema. Ad esempio, il danneggiamento o la distruzione di sistemi informatici di ospedali, caserme, ministeri è punito con la reclusione da due a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione (anche parziale) del funzionamento del sistema, la pena è la reclusione da tre a otto anni;
- **accesso abusivo a un sistema informatico o telematico (strettamente legato agli aspetti di riservatezza dei dati).** *L'articolo 615 ter* punisce chiunque si introduca in un sistema informatico o telematico protetto da misure di sicurezza (ovvero vi si mantenga all'interno contro la volontà espressa o tacita di chi ha il diritto di escluderlo). È il reato tipico degli **hacker** che attraverso la rete telefonica riescono a penetrare in diversi sistemi informatici collegati alla rete stessa. L'accesso abusivo a una banca dati protetta da misure di sicurezza (codici d'accesso, password, chiavi elettroniche ecc.), ad esempio, comporta pene fino a otto anni di reclusione;
- **detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.** *L'articolo 615 quater* punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo;
- **diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.** *L'articolo 615 quinquies* punisce chiunque diffonda, comunichi o consegni un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Per la diffusione di virus informatici si rischia la reclusione sino a due anni e una sanzione pecuniaria;
- **violazione, sottrazione e soppressione di corrispondenza.** Premesso che per corrispondenza si intende anche quella informatica o telematica, *l'articolo 616* del codice penale punisce chiunque prenda cognizione del contenuto di una corrispondenza a lui non diretta, ovvero sottragga o distrugga al fine di prenderne o di farne prendere cognizione ad altri una corrispondenza a lui non diretta, ovvero, in tutto o in parte la distrugga o sopprima. Questo quindi ha valore anche per la lettura fraudolenta di e-mail. I reati dell'*articolo 616* sono puniti con la reclusione fino a tre anni nell'ipotesi più grave;
- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.** *L'articolo 617 quater* punisce chiunque fraudolentemente intercetti comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. È ugualmente punito chiunque riveli, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni. Il reato punisce l'abusiva intromissione in comunicazioni in fase di trasmissione: si pensi a un fax inviato a un computer, oppure tra due sistemi informatici;



- **installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.** L'*articolo 617 quinquies* punisce chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte a intercettare, impedire, interrompere comunicazioni relative a un sistema informatico o telematico, ovvero intercorrenti tra più sistemi. Tale comportamento è sanzionato dal Codice penale, che prevede la reclusione da uno a quattro anni;
- **falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.** L'*articolo 617 sexies* punisce chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altrui danno, formi falsamente ovvero alteri o sopprima, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o intercorrenti tra più sistemi;
- **danneggiamento di sistemi informatici e telematici.** L'*articolo 635 bis* punisce chiunque distrugga, deteriori o renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui;
- **frode informatica.** L'*articolo 640 ter* punisce il reato di frode informatica. La frode informatica può realizzarsi attraverso l'alterazione del "funzionamento informatico e telematico" ovvero con l'intervento "senza diritto con qualsiasi modalità su dati, informazioni o programmi".  
Ad esempio, in caso di modifica dei risultati di un concorso pubblico, ottenuta alterando i dati contenuti in un sistema informatico, l'*articolo 640 ter* del Codice penale prevede la reclusione fino a cinque anni;
- **duplicazione ai fini di profitto.** È punito chiunque abusivamente duplichi, per trarne profitto, programmi per elaboratore o, ai medesimi fini, importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla SIAE. È il caso di un assemblatore di computer che installa sulle macchine vendute software senza licenza.

### 3.2 Il criminale informatico e il suo raggio d'azione

Nella tabella che segue presentiamo un riepilogo di alcuni tipi di crimini informatici con i relativi riferimenti legislativi che puniscono tali crimini, le tecniche di attacco utilizzate dal tipo di criminale e le conseguenze sociali provocate dal crimine.

TIPO DI CRIMINE	RIFERIMENTO LEGISLATIVO	CONSEGUENZE SOCIALI	OGGETTO DELLA TUTELA
Intrusioni informatiche con varie finalità (curiosità, spionaggio, operazioni economiche)	L. 547/93 art. 615 C.P.	La vittima prova disagio e vergogna, diffidenza verso i propri colleghi, si teme la reazione dei clienti.	Sicurezza delle operazioni, dei dati e delle informazioni personali.
Truffe a compagnie telefoniche	L. 547/93 art. 640 C.P.	Scarsa percezione del crimine. Diffidenza dei maggiori clienti verso le compagnie stesse.	Attività economica svolta dalle compagnie.
Utilizzo della rete per pedofilia	Proposta di L. 263, approvata nel giugno 1998	Cresce la diffidenza verso la Rete, aumentano i controlli ai siti, nascono rischi per privacy e diritto alla comunicazione.	Le vittime (sono reati contro la persona).
Duplicazione e traffico illecito di software	L. 518/92	Aumenta la difficoltà nel percepire tale costume come reato, aumentano i controlli a sorpresa, più attenzione per l'informatica "alternativa".	Attività economica degli sviluppatori delle software house.
Attentato alla rete o a singoli sistemi tramite virus	L. 547/93 art. 615 C.P.	Maggiore attenzione ai "contatti" tramite la Rete, i floppy disk, la provenienza dei programmi; sviluppo del mercato degli antivirus. Rischi di fobie collettive.	Tutto ciò che il virus danneggia.

TIPO DI CRIMINE	RIFERIMENTO LEGISLATIVO	CONSEGUENZE SOCIALI	OGGETTO DELLA TUTELA
Installazione e/o utilizzo di strumenti per intercettare, registrare, impedire, modificare comunicazioni informatiche e telematiche	L. 547/93 art. 617 C.P. (e altri)	Diffidenza verso qualsiasi tipo di comunicazione telematica, fobia del "Big Brother watching you" ("il Grande Fratello ti sta guardando"), rischi per la privacy e per lo sviluppo di alcuni servizi in Rete (ad esempio di tipo economico).	Sicurezza delle operazioni, dei dati e delle informazioni personali.

## 4 La legge sulla privacy

L'8 gennaio 1997, la Gazzetta Ufficiale ha pubblicato il testo della legge n. 675 sulla tutela delle persone e di altri soggetti rispetto al **trattamento dei dati personali** a favore della **protezione della privacy**. Con il decreto legislativo del 30/06/2003 è stato emanato il **codice in materia di protezione dei dati personali** che racchiude e raccoglie in modo organico la normativa inizialmente introdotta dalla legge 675.

L'evoluzione tecnologica ha reso possibile concentrazioni di raccolte di dati dai quali è possibile estrarre previsioni per l'adozione di ogni sorta di decisioni, che spaziano dalle scienze mediche all'andamento delle economie e dei mercati finanziari.

Appare dunque evidente il pericolo che si cela dietro il possesso e l'uso indiscriminato delle banche di dati.

Sono configurabili gravi violazioni dei diritti inalienabili dell'individuo (ad esempio, l'uso abusivo di informazioni personali potrebbe spingersi sino alla discriminazione per ragioni familiari, ideologiche o religiose).

Si tratta di una normativa destinata a incidere profondamente sulla responsabilità dei gestori di sistemi informatici, degli addetti alla sicurezza dei centri di *Electronic Data Processing (EDP)* e dei fornitori di connettività e di servizi Internet *Internet Service Provider (ISP)*.

La legge sulla *privacy* affronta il problema dei possibili **abusi** e delle violazioni del diritto alla riservatezza degli individui sotto un duplice profilo:

- impedire che un *archivio informatizzato* venga utilizzato per scopi diversi da quelli per cui è stato creato;
- sanzionare severamente (in sede penale) *il furto e la diffusione indebita* di informazioni custodite in archivi informatizzati.

Questa rivoluzione, che prevede il **trattamento dei dati** intimamente connesso al **consenso espresso** dell'interessato, si collega, per la parte che qui interessa, al concetto tradizionale di sicurezza informatica.

Sino a oggi, infatti, il compito del cosiddetto **titolare del trattamento dei dati** poteva limitarsi, nella maggior parte dei casi, alla valutazione dell'affidabilità tecnica del sistema.

Oggi, invece, il concetto di sicurezza si estende sino a comprendere l'integrità dei dati e la correttezza del loro utilizzo. La legge introduce, per la prima volta nel nostro ordinamento, un'**ipotesi di reato** per l'**omessa adozione delle misure** necessarie a garantire la sicurezza dei dati personali.

“ Per **dato personale** si intende qualunque informazione relativa a persona fisica, persona giuridica o ente, associazione che permette di identificare direttamente o indirettamente la persona o l'ente o condizione cui si riferisce. ”

All'interno della categoria dei dati personali distinguiamo tra:

- **Dati identificativi:** sono i dati personali che consentono di identificare direttamente una persona o un ente o un'associazione. Ad esempio, tramite nome, cognome, ragione sociale.

- **Dati giudiziari:** sono i dati personali idonei a rivelare informazioni relative a provvedimenti giudiziari in materia penale relativi a persone, enti o associazioni.
- **Dati sensibili:** sono i dati personali idonei a rivelare informazioni relative a:
  - origine razziale o etnica;
  - convinzioni filosofiche religiose o di altro genere;
  - opinioni politiche;
  - adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;
  - stato di salute e vita sessuale.

Premesso che tutti i dati personali sono tutelati dalla normativa sulla privacy, i dati giudiziari e quelli sensibili hanno una tutela più restrittiva. La pubblica amministrazione può liberamente trattare i dati personali per i fini istituzionali mentre, necessita di una apposita autorizzazione per il trattamento dei dati giudiziari e sensibili. Il trattamento dei dati sensibili non può avvenire senza il **consenso scritto** dell'interessato e previa autorizzazione del Garante.

Chiunque, essendovi tenuto, ometta di **adottare le misure necessarie per la sicurezza dei dati** è punibile, secondo il testo della legge, con la reclusione fino a due anni. Le pene, diminuite, si applicano anche al caso di condotta semplicemente colposa, cioè in caso di omissione dovuta a negligenza, imperizia o imprudenza del responsabile.

Le **misure minime di protezione** obbligatorie sono fissate dal codice in materia di protezione dei dati (art. 33) e prevedono che i dati siano custoditi in modo da ridurre al minimo i rischi di perdita, anche accidentale, dei dati o di intrusione non autorizzata nel sistema informativo automatizzato di trattamento non consentito.

Le principali **misure minime** per il trattamento dei dati personali con strumenti elettronici sono:

- **autenticazione** dell'utente che accede al sistema di elaborazione;
- utilizzo di un **sistema di protezione dei dati** (firewall, antivirus, ecc) rispetto ad accessi non autorizzati e a determinati programmi informatici che ne minacciano la sicurezza (virus, spyware, worm, ecc);
- adozione di procedure per il **back-up periodico** e di **ripristino** della disponibilità dei dati e dei sistemi;
- adozione e aggiornamento del **documento programmatico sulla sicurezza**.

Un **caso emblematico** di violazione del diritto alla privacy avvenne alla fine degli anni Novanta, quando fu reso pubblico un **baco** della piattaforma **Windows-Pentium**. Era infatti possibile leggere da programma il numero seriale del microprocessore. In questo modo, durante i collegamenti su Internet, era possibile riconoscere univocamente il computer (e quindi si presuppone il proprietario del computer) che si stava collegando in Rete.

#### 4.1 Documento programmatico sulla sicurezza

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati personali o di dati giudiziari deve redigere anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

- la precisione degli interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, delle responsabilità e delle modalità di aggiornarsi sulle misure minime;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura titolare;
- l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali relativi allo stato di salute e alla vita sessuale dagli altri dati personali.

#### 4.1 Le autorità

La massima autorità posta a tutela dei dati personali è il **Garante della privacy**, che ha compiti di:

- *vigilanza*;
- tenere il registro con le *notificazioni* del trattamento dei dati personali;
- emanare le *direttive*;
- dare *pareri*;
- accettare *segnalazioni* e ricevere denunce di violazioni;
- effettuare *attività ispettive*.

#### 4.2 Cookie e privacy

Come sappiamo, la maggior parte dei cookie rappresenta un valido sistema per migliorare la navigazione, ma possono però essere usati per scopi diversi. In particolare, la loro intercettazione potrebbe violare il diritto alla privacy (permettendo di ricostruire alcuni percorsi di navigazione Internet). Le versioni più aggiornate dei browser possono informare l'utente quando un server cerca di inviare un cookie, dandogli modo di scegliere se accettarlo o meno, alcuni browser consentono di stabilire politiche di accettazione o rifiuto dei cookies in base al server mittente o al contenuto stesso del cookie.

## 5 Gli aspetti contrattuali del commercio elettronico

Possiamo distinguere gli aspetti contrattuali del commercio elettronico in:

- **giuridici**;
- **fiscali**.

### 5.1 Gli aspetti giuridici del commercio elettronico

Nelle precedenti unità abbiamo visto una definizione di commercio elettronico, le varie sue forme, i sistemi di pagamento on line e la sicurezza dei sistemi di pagamento. Senza entrare nei dettagli delle norme contrattuali on line, possiamo dire che i **contratti telematici** rientrano, almeno nella legislazione italiana, nella **normativa per le vendite a distanza o a domicilio**. Il problema dei contratti on line è capire quando si tratta di una vendita effettuata in Italia o meno.

#### ESEMPIO

Se si acquista dal sito italiano della Microsoft si presuppone che il sito si trovi in Italia, ma è vero? Magari è solo il nome del dominio che fa credere si tratti di un sito italiano; il Web server potrebbe trovarsi ovunque. È quindi molto complesso capire quale sia la legge applicabile quando un "negozio giuridico" sia concluso tra interlocutori situati in Stati diversi.

Rimandiamo a trattazioni più tecniche per una dettagliata analisi sull'argomento.

#### 5.1.1 La tutela del consumatore nel commercio elettronico

Nelle operazioni di commercio elettronico appare evidente, in virtù della peculiarità e complessità del mezzo usato, la necessità di proteggere il consumatore – considerato contraente debole – da eventuali abusi del venditore.

In questo filone si inserisce la normativa sulla protezione del consumatore nei contratti a distanza, che prevede una serie di cautele per il consumatore nella fase antecedente la conclusione del contratto, obbligando il venditore a dare informazioni dettagliate (relative all'identità del fornitore). Va poi precisato che non basta registrare un dominio, ma si devono fornire i dati relativi a:

- *sede fisica e geografica* del soggetto;
- *caratteristiche essenziali* del bene o servizio;
- *prezzo*;
- *spese di consegna*;
- modalità di *pagamento*.

Tali informazioni devono essere fornite in modo chiaro e comprensibile, osservando i principi di buona fede e lealtà in materia di transazioni commerciali. È disposta, inoltre, l'estensione alla contrattazione telematica della disciplina dei contratti conclusi fuori dai locali commerciali (con qualche variazione), con il riconoscimento del **diritto di recesso** (esteso a **dieci giorni**), a favore dell'acquirente. Il fornitore inoltre deve eseguire l'ordine entro un termine massimo di trenta giorni, e in caso di mancata esecuzione ha l'onere di dare pronto avviso al cliente. È poi disposto che, in alcuni casi, il diritto di recesso non operi, ad esempio in occasione di vendite all'asta, contratti di fornitura di servizi relativi all'alloggio e trasporti, servizi finanziari.

### 5.1.2 Aspetti della firma digitale

Grazie all'introduzione della **firma digitale**, sia il commercio elettronico sia qualunque altro tipo di contrattazione on line possono essere sottoscritte con validità di legge.

### 5.1.3 La normativa di riferimento

Nella tabella che segue sono raccolte alcune disposizioni che riguardano il commercio elettronico nella normativa italiana.

Decreto legislativo	
15 gennaio 1992 n. 50	Attuazione della direttiva n. 85/577CEE in materia di contratti negoziati fuori dei locali commerciali
31 marzo 1998 n. 114 (art. 18)	Riforma della disciplina relativa al settore del commercio elettronico a norma dell'articolo 4, comma 4, della legge 15 marzo 1997.
22 maggio 1999 n. 185	Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza.
9 aprile 2003 n. 70	Attuazione della direttiva 200/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno. Le società che vendono on-line devono fornire sui siti informazioni utili alla loro identificazione e rintracciabilità. Riguarda, quindi, aspetti legati alla trasparenza ovvero "so da chi compro" e "so cosa sto comprando".

Allo scopo di accrescere la fiducia dei consumatori nell'acquisto on-line e offrire loro una tutela effettiva in caso di adempimento, è intervenuto il regolamento del Consiglio dell'Unione Europea del 22 dicembre 2000, n. 44, che riguarda la competenza giurisdizionale e il riconoscimento ed esecuzione delle decisioni in materia civile e commerciale nell'Unione Europea.

Tale regolamento prevede che chi compra un prodotto on-line da uno stato membro può citare l'azienda titolare del sito nel Paese del proprio domicilio e non in quello in cui l'a-

zienda è domiciliata. D'altra parte, se l'acquirente dovesse citare l'azienda nel Paese in cui è domiciliata, ne deriverebbero ovvie conseguenze negative.

Un acquirente di Genova, ad esempio, se acquista in Germania può fare la causa a Genova e la sentenza è valida in Germania.

L'azienda deve, invece, fare causa necessariamente nella sede del domicilio dell'acquirente.

## 5.2 Gli aspetti fiscali del commercio elettronico

Sotto il profilo fiscale, in un contesto oggi caratterizzato dall'assenza di principi regolatori internazionali, il commercio elettronico è rilevante ai fini dell'IVA, delle imposte doganali e della tassazione sui redditi.

Le principali conclusioni alle quali è giunta l'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) possono riassumersi nella raccomandazione di creare un **sistema fiscale neutrale**, in modo da non influenzare, ostacolare o avvantaggiare oltremodo lo sviluppo del commercio elettronico.

Tralasciando le problematiche derivanti dall'applicazione di tali nuovi principi (la maggior parte di essi è ancora in via di formazione) al sistema impositivo nazionale, esaminiamo sommariamente le ripercussioni degli acquisti effettuati via Internet sull'attuale quadro normativo italiano.

### 5.2.1 L'applicazione dell'IVA

L'IVA, com'è noto, è un'imposta che colpisce sia le cessioni di beni sia le prestazioni di servizi. Questa interessa il commercio elettronico solo se si considera

“ l'acquisto di beni materiali che successivamente vengono fisicamente recapitati attraverso il servizio postale o i corrieri (**commercio elettronico indiretto**) oppure l'acquisto e la spedizione on line di beni e servizi immateriali come il software (**commercio elettronico diretto**). ”

### 5.2.2 Il commercio elettronico indiretto

Il **commercio elettronico indiretto** consta di un semplice ordinativo di spesa, cui segue una regolare fattura attestante la vendita. L'ordine viene quindi evaso attraverso i tradizionali canali di consegna. Ai fini dell'applicazione dell'IVA:

- se il venditore è un soggetto residente in Italia e il bene si trova nel territorio dello Stato, l'acquisto *sconta l'IVA nel territorio nazionale*, poiché è qui imponibile;
- qualora, invece, il venditore sia un operatore residente in uno Stato membro dell'Unione Europea e il bene provenga da uno Stato dell'Unione, si configura un *acquisto intracomunitario*;
- se il venditore, infine, è un soggetto extracomunitario e il bene proviene da uno Stato non appartenente all'Unione Europea, l'operazione deve considerarsi un'*importazione* (l'IVA relativa andrà versata, insieme ai dazi, in dogana).

### 5.2.3 Il commercio elettronico diretto

Un'altra modalità per ottenere un bene via Internet si realizza quando si acquista un bene immateriale, ossia un bene che non necessita, per essere trasferito, di un supporto fisico, ma che può essere trasferito per via telematica.

È ciò che si verifica, ad esempio, per i programmi software scaricabili direttamente dai siti Web. In questo caso si pone il dubbio se ciò che viene trasmesso possa essere qualificato come cessione di un bene o, piuttosto, come prestazione di servizi.

Attualmente, secondo l'Amministrazione Finanziaria, il *software standardizzato* deve essere considerato alla stregua di un qualsiasi bene materiale. Un *software personalizzato* in base alle esigenze del committente deve, invece, qualificarsi come prestazione di un servizio. Sotto il profilo fiscale:

- se colui che vende il programma è un *operatore italiano*, sia che l'operazione si qualifichi quale cessione di beni o prestazione di servizi, si tratta, in entrambi i casi, di un'operazione imponibile ai fini IVA;
- se il venditore è un *operatore residente in un Paese dell'Unione Europea*, è opportuno distinguere due casi:
  - se il programma software è *standardizzato* l'operazione è da considerarsi acquisto intracomunitario;
  - se il programma è un software *personalizzato* l'imponibilità dell'operazione è in territorio italiano;
- se il cedente è *residente fuori dall'Unione Europea* si tratta di un'importazione:
  - il software *standardizzato* sconta l'IVA in dogana (sul valore complessivo del supporto, comprendente anche il prezzo dei dati e delle istruzioni ivi contenute);
  - per il software *personalizzato* la base imponibile è costituita dal valore della prestazione di servizi acquisita.

È di immediata evidenza, soprattutto in quest'ultimo caso, la difficoltà cui va incontro colui che opera mediante Internet che, dopo aver scaricato un programma da un sito, dovrebbe – secondo le attuali disposizioni di legge – recarsi in dogana per regolarizzare l'acquisto. Rilevanti appaiono anche le potenzialità evasive del commercio elettronico, se solo si considera la possibilità di effettuare transazioni anonime o sotto pseudonimo, con l'eventualità di utilizzare la moneta elettronica, che permette di effettuare il pagamento per via telematica senza passare attraverso gli intermediari finanziari o bancari. Ovviamente, il legislatore sta ponendo rimedio a ogni questione.

#### 5.2.4 L'imposizione sui redditi

I proventi derivanti dalle cessioni di beni e prestazioni di servizi effettuate via Internet costituiscono reddito imponibile rispettivamente ai fini IRPEF e IRPEG.

L'applicazione della normativa nazionale vigente risulta, peraltro, di difficile attuazione sul piano pratico, innanzitutto perché è ardua l'individuazione di una chiara e precisa relazione tra i computer, l'utente del servizio, il fornitore del servizio e gli indirizzi Internet.

Facile, inoltre, è la possibilità di eludere l'obbligo fiscale della registrazione su libri e scritture contabili, visto che tutte le transazioni avvengono elettronicamente.

## CONOSCENZE di BASE

### VERO O FALSO

- |   | V                        | F                        |
|---|--------------------------|--------------------------|
| 1. Secondo la legislazione italiana il software è brevettabile.   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Secondo la legislazione statunitense il software è brevettabile.   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Il software, secondo la legislazione italiana prima della legge 518/92, era considerato un'opera letteraria.               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. L'algoritmo è brevettabile poiché è opera dell'ingegno.  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. La decompilazione è sempre vietata per legge.  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Software libero e freeware hanno il medesimo significato.  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Il software commerciale può essere anche proprietario.   | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Il software libero può essere anche commerciale.   | <input type="checkbox"/> | <input type="checkbox"/> |
| 9. Esiste software non commerciale e non libero.  | <input type="checkbox"/> | <input type="checkbox"/> |
| 10. I diritti d'autore morali per lo shareware cessano dopo 20 anni.  | <input type="checkbox"/> | <input type="checkbox"/> |
| 10. Che differenza c'è tra software con permesso d'autore e senza?  |                          |                          |
| 11. Qual è il software soggetto a tutela del diritto d'autore e quale non lo è?   |                          |                          |
| 12. Il software libero, se modificato, cosa può diventare?  |                          |                          |
| 13. Per il diritto penale è possibile applicare l'interpretazione in via analogica?   |                          |                          |
| 14. Perché la legge n. 547 del 1993 è un passaggio importante nella normativa italiana sui crimini informatici?               |                          |                          |
| 15. Nell'ambito di quale reato informatico, contemplato dalla legge n. 547 del 1993, ricade la violazione sulla riservatezza? |                          |                          |
| 16. Nell'ambito di quale reato informatico, contemplato dalla legge n. 547 del 1993, ricade la diffusione di virus?           |                          |                          |
| 17. Qual è l'oggetto di tutela della legge sulla privacy?   |                          |                          |
| 18. Quali sono i compiti del Garante della privacy?   |                          |                          |
| 19. Perché i cookies possono violare la privacy?  |                          |                          |
| 20. Qual è la maggior problematica dei contratti telematici nel commercio elettronico?  |                          |                          |
| 21. In cosa consistono gli aspetti fiscali del commercio elettronico?   |                          |                          |

### QUESITI

1. Come viene definito il "diritto d'autore"?
2. Qual è l'oggetto della tutela del diritto d'autore del software?
3. Qual è la prima legge di riferimento sul diritto d'autore del software?
4. Come sono definiti, secondo la normativa italiana, i programmi per calcolatore?
5. In quale decreto legislativo è stata inserita la tutela delle banche dati?
6. Quali sono i vantaggi della registrazione del software presso la SIAE?
7. Parlando di diritto d'autore, qual è la differenza tra diritto morale e diritto di utilizzazione economica? Quando cessano tali diritti?
8. Cosa dicono le due filosofie opposte del mondo del software?
9. Che differenza c'è tra software libero e software con permesso d'autore?

### COMPLETAMENTI

1. I diritti morali sono strettamente connessi alla ..... dell'autore. Il diritto di utilizzazione economica consente invece di effettuare qualsiasi ..... sul software.
2. La licenza GPL è un caso particolare di ..... Il software semilibero è software ..... (quindi non è rilasciato con i sorgenti), ma è distribuito ..... permesso per i privati di essere usato, copiato, distribuito e modificato (includere le versioni distribuite con modifiche) ma senza .....
3. L'articolo ..... punisce chiunque fraudolentemente intercetta comunicazioni relative a un ..... ovvero le impedisce o le interrompe. L'articolo ..... punisce chiunque altera o sopprime il contenuto delle comunicazioni tra ..... due .....



# SCHEDA di AUTOVALUTAZIONE

## Per la valutazione delle competenze personali dello studente

Con questa scheda puoi autovalutare il tuo livello di acquisizione delle conoscenze e delle abilità presentate nell'Unità di apprendimento.

### CONOSCENZE DI BASE

Livello

1 2 3 4

• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### ABILITÀ DI BASE

Livello

1 2 3 4

• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Xxxxxxx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Legenda:** 1 = con molta incertezza 2 = con qualche difficoltà 3 = con sufficiente sicurezza 4 = con sicurezza