DIEGO MARRA

INTERNET
COME PROTEGGERE LA PROPRIA ATTIVITA'

Sommario

INTRODUZIONE

Prima di iniziare la lettura è necessario considerare che sebbene questo libro sia stato scritto con un linguaggio accessibile, evitando volutamente di menzionare i riferimenti normativi, ho scelto di inserire un minimo di terminologia tecnico-giuridica, al fine di rendere comprensibili alcuni passaggi fondamentali, e soprattutto perché in ambito legale è pressoché impossibile eliminare completamente il linguaggio tecnico.

Sicuramente le nozioni tecniche e giuridiche esposte appariranno meno romanzesche, ma il lettore attento ed interessato le coglierà come passaggi importanti per la propria formazione professionale e personale.

Alla realizzazione di questo libro, sono stato spinto da una duplice ragione. Le ragioni di cui parlo sono costituite da alcuni argomenti, tra i più importanti, la Privacy e Internet; argomenti ormai entrati nel linguaggio comune, e che necessitano di una normativa sempre più capillare. Effettivamente, questi due argomenti sono molto dibattuti in ambito forense, per cui se da una parte il legislatore (Italiano ed Europeo) si avventura in un territorio inesplorato poiché non riesce a trovare dei confini che traccino la geografia di argomenti così importanti che ne definiscano gli ambiti di applicazione; dall'altra, le leggi a tutela di questo bene tanto decantato sono però vive e vegete.

Aumenta sempre di più anche l'attenzione rivolta a Internet. Difatti, negli ultimi cinque anni, gli acquisti, realizzati sul web, sono cresciuti ogni anno del 20%, e i numeri sono destinati a salire; proprio perché il web favorisce la crescita costante dell'economia di mercato, a scapito di quella vecchia e tradizionale.

A questo punto è lecito pensare che anche su internet esista una normativa che vada a tutelare sia il semplice navigante sia il titolare di un'attività online.

Nella mia attività sempre più spesso mi vengono richiesti consigli su come tutelarsi e rendere sicura la propria attività on-line. Quotidianamente affronto argomenti quali: privacy e riservatezza, copyright e diritti d'autore, domain name, SIAE, reati informatici, commercio elettronico.

A conclusione di questa breve introduzione, l'obiettivo di questo lavoro è di dare dei consigli significativi a quanti già hanno un'attività online e vogliono tutelarsi dal punto di vista legale per rendere tranquilla e sicura la propria attività. Questo testo si rivelerà utile anche a tutti coloro che desiderano iniziare un'attività online e che

cercano dei consigli utili su come tutelarsi dal punto di vista normativo. E' infine rivolta a tutti coloro che per qualsiasi ragione necessitano di avere informazioni inerenti la compagine normativa riguardante il web.

CAPITOLO PRIMO (privacy)

1. CODICE DELLA PRIVACY SISTEMATICA

Il codice della privacy è attualmente previsto dal D.Lgs. n. 196 del 30 giugno 2003 ed è suddiviso in tre parti:

A) Disposizioni generali

Sono le norme rivolte alle varie figure coinvolte nelle operazioni, quali: titolare, responsabile, interessato;

B) Disposizioni relative a specifici settori

Sono le disposizioni che disciplinano il trattamento dei dati in ambito giudiziario, sanitario, lavorativo, giornalistico e nelle comunicazioni;

C) Tutela dell'interessato e sanzioni

E' la parte dedicata alla tutela amministrativa e giurisdizionale, comprende un titolo intero dedicato alle sanzioni amministrative e agli illeciti penali.

In appendice al codice sono inoltre presenti tre allegati:

Allegato A: presenta un codice di deontologia, a sua volta suddiviso in tre parti;

A1 trattamento dati personali nell'esercizio dell'attività giornalistica;

A2 - trattamento per scopi storici;

A3 - trattamento per scopi statistici in ambito SISTAM.

Allegato B: disciplinare tecnico in misure minime di sicurezza

Allegato C: trattamento non occasionale in ambito giudiziario

2. DISPOSIZIONI GENERALI: PRINCIPI GENERALI

Il Codice della Privacy si apre con un principio semplice e chiaro, "chiunque ha diritto alla protezione dei dati personali che lo riguardano".

Lo scopo della norma è che i dati personali vanno tutelati qualunque sia il trattamento al quale sono sottoposti.

Per comprendere nella sua totalità il significato e la forza di questa espressione basti pensare che la tutela dei dati personali si riscontra anche nell'art. 2 della Costituzione.

Il codice della privacy fissa dei principi generali che governano la sua intera struttura, ossia che il trattamento e' lecito se sussiste una ragione che lo giustifica, come ad esempio un rapporto contrattuale, ed inoltre la finalità del trattamento deve essere esplicita e legittima.

I dati devono essere utilizzati solo in caso di necessità, oltre al fatto che tutti i dati personali e il relativo trattamento deve riferirsi alla finalità che si persegue e non deve eccedere in altre finalità.

3. TITOLARE, INTERESSATO E RESPONSABILI DEL TRATTAMENTO

Per una migliore comprensione della materia giuridica, è necessario chiarire alcune figure ed espressioni lessicali contenute nel codice della privacy.

Per Trattamento si intendono le "*operazioni quali raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, comunicazione, diffusione, cancellazione, distruzione"* anche se non registrati in una banca dati".

Il trattamento può riguardare anche una sola delle operazioni sopra elencate e senza che si ricorra all'ausilio di strumenti informatici.

***IL TITOLARE*:** è colui che esegue il trattamento dei dati personali (es. una società che invia pubblicità tramite e-mail, perché è stata autorizzata da un soggetto al trattamento dei dati).

***L'INTERESSATO*:** è il Soggetto a cui i dati si riferiscono, cioè il *"dominus"* del dato personale. L'interessato può autorizzare il Titolare al trattamento e sfruttamento dei dati che lo riguardano.

Il soggetto interessato ha il diritto di accedere ai dati personali che si riferiscono alla sua persona per esercitare gli altri diritti previsti. Tra i più importanti ricordiamo:

a) il diritto di integrare i propri dati con l'aggiornamento o la rettifica;

b) il diritto alla cancellazione dei dati personali in blocco;

c) l'attestazione che le operazioni di cui alla lettera a) e b) sono stati portate a conoscenza ai soggetti ai quali i dati sono stati diffusi;

d) il diritto di conoscere la finalità del trattamento;

e) il diritto di avere gli estremi identificati del titolare;

Nello specifico se l'Interessato esercita il proprio diritto d'accesso o gli altri diritti che gli sono riconosciuti, il Titolare ha l'obbligo di fornire riscontro entro 15 gg. dal ricevimento dell'istanza. Qualora a seguito dell'istanza dell'Interessato, non vi fosse un riscontro completo o se quest'ultimo risulti incompleto, i diritti potranno essere fatti valere innanzi all'Autorità Giudiziaria o in alternativa all'Autorità Garante.

RESPONSABILE DEL TRATTAMENTO: è la Persona fisica o giuridica, oppure l'Ente che decide del trattamento e sugli strumenti utilizzati può nominare uno o più soggetti *"responsabili del trattamento dei dati"* con poteri determinati dall'atto di nomina.

AMMINISTRATORE DI SISTEMA: è colui che funge da ausiliario del titolare. E' un soggetto di pari livello al Responsabile del trattamento. I suoi compiti sono rivolti alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati i trattamenti dei dati personali. Si tratta di una figura affidabile con elevate competenze tecniche. *La loro identità deve essere resa nota tramite menzione nel DPS (documento programmatico sicurezza).*

Le attività svolte dal Responsabile del Trattamento e dall'Amministratore del Sistema, vanno verificate mediante controllo, almeno annuale, con i dovuti accorgimenti.

Tutti coloro che verranno a conoscenza diretta dei dati (es. impiegati), sono denominati incaricati. A questi vanno impartite precise istruzioni esecutive da parte del Titolare del trattamento o dal Responsabile del trattamento.

4. ADEMPIMENTI VERSO IL GARANTE

Il Garante è una figura che spesso ritroviamo in TV e nei quotidiani, è la figura a garanzia dei diritti della privacy. In particolare impone a chiunque stia trattando dei dati personali l'obbligo di disporre di due adempimenti che devono essere esercitati a garanzia e protezione dei dati personali:

*LA **NOTIFICAZIONE:*** è una dichiarazione attraverso la quale il titolare (chi sta trattando i dati) comunica al Garante l'esistenza di un'attività di trattamento dei dati personali.

Attualmente la notificazione è prevista solo per alcuni casi tassativamente previsti e cioè:

a) i dati genetici, biometrici o dati che indicano la posizione geografica di persone mediante una rete di comunicazione elettronica;

b) i dati che rilevano lo stato di salute delle persone, vita sessuale, indagini epidemiologiche, malattie mentali, infettive, diffusive, sieropositività, trapianto di organi;

c) i dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro;

d) i dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo, la personalità dell'interessato le scelte di consumo, oppure dati che servono per monitorare i servizi di comunicazione utilizzati;

e) i dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato o altre ricerche campionarie;

f) i dati registrati nelle opportune banche dati, le quali sono gestite con strumenti elettronici adatti che consentono di ridurre il rischio d’insolvibilità economica, e contribuiscono a gestire meglio la situazione patrimoniale;

La notificazione deve essere fatta una sola volta per tutti i trattamenti all'inizio dell'attività, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare;

E' inoltre valida solo la notificazione trasmessa attraverso il sito del Garante compilando un apposito modulo.

OMESSA O INSUFFICIENTE NOTIFICAZIONE, O FALSITA' NELLE DICHIARAZIONI E NOTIFICAZIONI - Le conseguenze per omessa od incompleta notificazione sono molto gravi, infatti sia nell'uno o nell'altro caso è prevista la sanzione pecuniaria amministrativa che varia dai 20 a 120 mila euro e il reato di falsità è punito con la reclusione da 6 mesi a 3 anni.

LA RICHIESTA DI AUTORIZZAZIONE PER I DATI SENSIBILI - Per quanto riguarda i dati sensibili il codice adotta particolari accorgimenti, infatti possono essere trattati solo con il consenso scritto dell'Interessato e con l'autorizzazione da parte del Garante, salvo che si tratti di:

1) dati relativi agli aderenti di confessioni religiose;

2) fatti riguardanti aderenti ad associazioni sindacali;

Ricevuta la richiesta il Garante comunica la decisione adottata entro 45 giorni, decorsi i quali la mancata pronuncia equivale a rigetto.

Il Garante con il provvedimento di autorizzazione prescrive gli accorgimenti che il Titolare è tenuto ad adottare.

AUTORIZZAZIONI GENERALI - Dato l'alto numero di soggetti interessati, solitamente a gennaio di ogni anno, il sito del Garante pubblica la concessione delle autorizzazioni generali a speciali categorie di Titolari o di trattamenti. In particolare il Garante autorizza d'ufficio con provvedimenti di carattere generale.

Attualmente le principali autorizzazioni generali riguardano il trattamento dei seguenti dati sensibili:

- dati sui rapporti di lavoro;

- dati sullo stato di salute e la vita sessuale;

- dati riguardanti organismi di tipo associativo e fondazioni;

- dati sui liberi professionisti;

- dati su diverse categorie di titolari;

- dati su investigatori privati;

- dati a carattere giudiziario da parte di privati, enti pubblici economici e soggetti pubblici;

***SANZIONI**:* Il legislatore ha previsto, per quanto riguarda le violazioni in tema di trattamento dei dati, sanzioni molto elevate che prevedono la reclusione da 1 a 3 anni, "*se dal fatto deriva nocumento"* (danno) e se sussiste *"il fine di trarne per se o per altri profitto o di recare ad altri un danno"* (dolo specifico).

4.1 GLI ADEMPIMENTI VERSO GLI INTERESSATI

I principali destinatari della tutela sono gli Interessati, verso i quali il legislatore ha stabilito dei precisi adempimenti che i titolari del trattamento devono rispettare e sono:

***FORNIRE L'INFORMATIVA*:** E' una comunicazione che può essere orale oppure scritta, che informa l'interessato sui soggetti che effettueranno il trattamento, attraverso quali modalità avverrà e per quali finalità. I contenuti obbligatori della comunicazione sono:

- finalità e modalità del trattamento;

- natura facoltativa e obbligatoria del conferimento dati;

- conseguenze di un eventuale rifiuto a rispondere;

- i soggetti o categorie ai quali possono essere inviati i dati o averne conoscenza;

- estremi identificativi del titolare;

- diritti dell'interessato;

La forma su come elaborare il contenuto dell'informativa è lasciata alla libertà per cui non esistono preconfezionati. Il titolare dei dati elabora l'informativa come riterrà opportuno e secondo le proprie esigenze. La forma scritta è comunque fortemente preferibile, visto che costituisce una prova certa.

OMESSA O INIDONEA INFORMATIVA - La violazione dell'"obbligo di informativa" è sanzionata da 6 a 36 mila euro;

DIRITTO DI ACCESSO - L'interessato ha il diritto di essere informato su tutto ciò che concerne il trattamento dei propri dati.

PREVENTIVA RICHIESTA DI CONSENSO - Il consenso, per essere validamente considerato, deve essere: espresso, libero, specifico, informato, e documentato per iscritto. Per i dati sensibili il consenso salvo le esenzioni previste va sempre manifestato in forma scritta.

DEROGHE ALL'OBBLIGO DI MANIFESTAZIONE DEL CONSENSO – Il consenso espresso è escluso nel caso di "obblighi normativi"; quali il trattamento necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato. Il trattamento riguardante dati contenuti in "pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Il trattamento per l'incolumità fisica di un terzo, investigazioni difensive, diritti in sede giudiziaria.

Il titolare che procede senza consenso "se dal fatto deriva nocumento" è punito con la reclusione da sei a diciotto mesi oppure "se il fatto consiste nella comunicazione o diffusione" la pena è della reclusione da sei a ventiquattro mesi.

5. ADEMPIMENTI INTERNI O ORGANIZZATIVI

MISURE TECNICHE **-** Oltre a quanto sopra riportato vi sono una seria di norme che disciplinano le cosiddette "misure di sicurezza". Si tratta di una serie di misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano il livello minimo di protezione normativamente richiesto rispetto ai rischi di: perdita di dati, accesso non autorizzato o trattamento non consentito o non conforme.

Se questa tipologia non viene rispettata si concretizza la responsabilità penale di omissione delle misure minime con conseguente sanzione detentiva fino a due anni.

La medesima disposizione prevede il ravvedimento operoso, che consiste in una prescrizione dell'Autorità garante nei confronti dell'autore del reato il quale entro 6 mesi deve regolarizzare la non conformità. Nei 60 gg. successivi allo scadere del termine, se risulta l'adempimento della prescrizione, l'autore del reato è ammesso a pagare una somma pari al quarto della sanzione stabilita per la violazione amministrativa. L'adempimento è il pagamento estinguono il reato.

Le misure minime non sono in grado di garantire la sicurezza dei sistemi utilizzati per il trattamento dei dati personali e di conseguenza il loro rispetto non è sufficiente a liberare da ogni responsabilità il titolare del trattamento. Le misure devono essere idonee pertanto ad evitare il danno che dal trattamento potrebbe derivare all'interessato.

Il titolare che non garantisce misure idonee al trattamento può incorrere in una responsabilità civile e di conseguenza essere obbligato a risarcire il danno, disciplinato alla stregua dell'art. 2050 cc (responsabilità per l'esercizio di attività pericolose). Colui che provochi danni a terzi nello svolgimento di un'attività

pericolosa "per sua natura e per i mezzi adoperati", esercita tale tipo di attività e deve risarcire il danno, inoltre possiede la facoltà di scagionarsi dimostrando di aver adottato tutte le misure idonee ad evitare l'evento dannoso. Si tratta di una presunzione speciale di colpa a carico del titolare del trattamento.

Per onere probatorio si intende il fornire la prova di aver adottato tutte le misure idonee ad evitare il danno. Di solito spetta a colui che agisce in giudizio. Nel caso specifico l'art. 15 del Codice sposta l'onere probatorio a carico del convenuto, in tal caso la prova deve essere dimostrata da chi ha subito il danno.

5.1 L'ALLEGATO B

Le misure minime di sicurezza prevedono l'autenticazione informatica. Di conseguenza il trattamento dei dati personali sarà consentito solo agli incaricati muniti di credenziali di autenticazione. Le credenziali sono costituite da un codice, per l'identificazione dell'incaricato, associato ad una parola chiave segreta, conosciuta dall'incaricato stesso il quale adotta tutte le cautele necessarie per assicurare la segretezza. Il titolare al primo utilizzo dovrà modificarla, se il trattamento riguarda dati comuni modificarla ogni sei mesi, oppure ogni tre mesi se riguarda dati sensibili e giudiziari.

E' prevista inoltre l'adozione di un sistema di autorizzazione per gli incaricati, ai quali siano stati attribuiti differenti profili di accesso ai dati.

L'Allegato B impone di limitare l'accesso ai soli dati necessari alla realizzazione delle operazione di trattamenti per cui sono previsti. Altro aspetto riguarda la protezione dei dati personali contro l'intrusione, e dell'azione di programmi diretti a danneggiare o interrompere un sistema informatico. A tal proposito l'art. 615 quinquies c.p., disciplina la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. L'Allegato B al punto 16 prevede un aggiornamento semestrale.

Gli attacchi ai dati vengono messi in atto da soggetti fisici abili con i sistemi informatici e telematici.

Il codice della privacy disciplina anche il back-up dei dati, ovvero il salvataggio delle informazioni personali trattate dal titolare. La disposizione impone l'adempimento in argomento con frequenza almeno settimanale su supporti rimovibili appositamente custoditi.

DISASTER RECOVER - All. B - Prevede misure speciali e idonee per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti

elettronici. Questo avviene in tempi certi compatibili con i diritti degli interessati non superando i sette giorni.

OBBLIGO IMPLICITO - Al fine di ottenere una maggiore tutela si deve procedere periodicamente allo svolgimento di testi diretti alla simulazione di avarie del sistema.

L'adozione di tutte le misure sopra descritte richiede competenze tecniche, il soggetto che ricopre questo ruolo è l'amministratore di sistema. Si tratta di una figura di recente introduzione che viene nominata dal titolare, previa valutazione dell'esperienza, capacità e affidabilità. Il soggetto può essere anche esterno.

Il DOCUMENTO PROGRAMMATICO DELLA SICUREZZA (DPS) – Attualmente non obbligatorio ma sempre preferibile la sua redazione, è la misura di sicurezza maggiormente conosciuta nell'Allegato B. Deve essere adottato entro il 31 marzo di ogni anno da coloro che si occupano, mediante l'ausilio di strumenti elettronici, del trattamento dei dati sensibili e/o dei dati giudiziari. E' preferibile, nonché opinione comune, che i titolari del trattamento dati provvedano alla redazione del DPS ogni anno a prescindere dalla tipologia dei dati trattati.

Il "Decreto Sviluppo" convertito in L. 106/2011 ha approvato importanti novità sulla redazione del DPS rispetto alla Legge 133/2008, ove in questo caso era prevista l'esenzione per la trattazione dei dati sensibili riguardanti lo stato di salute o malattia dei propri dipendenti e collaboratori, senza indicare la diagnosi, oppure l'esenzione per i dati concernenti l'adesione di soggetti ad organizzazioni sindacali. Ad oggi la redazione del DPS è estesa a tutti i dati sensibili e giudiziari.

Quanto al contenuto, nel DPS si devono descrivere tutti gli accorgimenti e le misure di sicurezza adottate e che si adotteranno, al fine di ottenere una riduzione dei rischi derivanti dal trattamento dei dati personali.

In particolare le informazioni essenziali che devono comparire nel DPS riguardano:

A) i compiti e le responsabilità dei soggetti incaricati al trattamento;

B) l'analisi dei rischi; indicando tutte le misure adottate al fine di garantire l'integrità e la disponibilità dei dati; nonché la protezione delle aree e dei locali in relazione alla loro custodia e accessibilità; l'individuazione delle modalità di ripristino dei dati qualora vengano distrutti o danneggiati.

C) interventi formativi in tema di analisi dei rischi che incombono sui dati; criteri per la separazione dei dati sensibili da quelli comuni;

D) criteri per l'adozione delle misure minime di sicurezza in caso di trattamenti di dati affidati all'esterno della struttura;

La mancata predisposizione del DPS costituisce contravvenzione ed è punita con l'arresto fino a due anni. Il documento va conservato presso la sede del titolare e seppure non vi è una prescrizione di legge sarebbe preferibile avesse una data certa in modo da poter dimostrare che è stato redatto entro la scadenza prevista dal Codice della privacy.

Per l'acquisizione di una data certa, si possono suggerire le seguenti modalità:

1) auto-prestazione presso gli uffici postali con apposizione del timbro datario della Posta direttamente sul documento, anziché sulla busta, previa apposizione di francobollo di posta prioritaria e la dicitura auto-prestazione;

2) registrazione del documento presso un ufficio pubblico (es. Ag. Entrate);

3) registrazione del documento presso un pubblico ufficiale (notaio);

4) menzione dell'avvenuta adozione del DPS in un'assemblea o consiglio direttivo.

6. SISTEMI DI VIDEOSORVEGLIANZA (Provv. 8 aprile 2010)

Con il Nuovo Provvedimento dell’8 aprile del 2010 l'autorità garante per la privacy è intervenuta per il settore della videosorveglianza.

Il nuovo Testo tiene conto dell'aumento massiccio dei sistemi di videosorveglianza per la prevenzione, accertamento, repressione dei reati, sicurezza pubblica, tutela della proprietà, controllo stradale, etc.

Nel provvedimento l'Autority tiene in considerazione altri interventi, tra i quali il *"Decreto Antistupro 23 febbraio 2009"*, nonché norme statali e regionali che hanno introdotto forme di incentivazione economica a favore delle amministrazioni pubbliche e di soggetti privati al fine di incrementare e migliorare il servizio di videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

Con il Nuovo Provvedimento dell’8 aprile del 2010 l'autorità garante per la privacy è intervenuta per il settore della videosorveglianza.

Il nuovo Testo tiene conto dell'aumento massiccio dei sistemi di videosorveglianza per la prevenzione, accertamento, repressione dei reati, sicurezza pubblica, tutela della proprietà, controllo stradale, etc.

Nel provvedimento l'Autority tiene in considerazione altri interventi, tra i quali il *"Decreto Antistupro 23 febbraio 2009"*, nonché norme statali e regionali che hanno introdotto forme di incentivazione economica a favore delle amministrazioni pubbliche e di soggetti privati al fine di incrementare e migliorare il servizio di videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

6.1 PRINCIPI GENERALI

In apertura il provvedimento contiene una precisazione che riconduce la videosorveglianza all'attività di trattamento dei dati personali.

Il principio di finalità è ancora una volta il primo a essere invocato e nel farlo il Garante individua alcune categorie di trattamenti che rappresentano le principali applicazioni di videosorveglianza, e cioè:

1) Sicurezza Urbana, ordine e sicurezza pubblica, prevenzione, accertamento o repressione dei reati;

2) protezione della proprietà;

3) rilevazione, prevenzione, controllo delle infrazione da parte dei soggetti pubblici;

4) l'acquisizione delle prove;

Il trattamento con i sistemi di videosorveglianza deve essere improntato al generale rispetto dei diritti e della libertà, principi fondamentali degli interessati.

Si possono riprendere persone identificabili solo se, non siano utilizzabili esclusivamente dati anonimi (principio di necessità). Ad esempio nel caso di monitoraggio sul traffico, sono consentite soltanto riprese generali, che escludano la possibilità di rendere identificabili le persone.

E' inoltre imposto un trattamento pertinente e non eccedente rispetto alle finalità perseguite, ad esempio nella scelta delle modalità di ripresa e dislocazione delle telecamere.

Inoltre tutti quelli che transitano dalla zona video-sorvegliata devono essere informati della presenza di telecamere attraverso l'affissione di speciali cartelli, i quali devono

essere chiaramente visibili ed esplicativi degli elementi previsti dall'art. 13 del D.Lgs. n. 196/03, anche quando il sistema di videosorveglianza è attivo in orario notturno.

Il cartello deve essere collocato prima della telecamera, deve essere chiaro e visibile in ogni condizione di illuminazione ambientale e può inglobare un simbolo di esplicita comprensione.

L' Art. 3.1.1 esime dell'obbligo di fornire una preventiva informativa agli interessati, coloro che effettuano il trattamento anche sotto forma di suoni e immagini, per le finalità indicate nell' art. 53 del Codice sulla Privacy.

Si tratta dei trattamenti svolti dalle Forze di Polizia, organi di sicurezza e altri soggetti pubblici che si occupano della prevenzione, dell'accertamento e repressione dei reati.

Va precisato inoltre che i titolari beneficiari dell'esenzione dall'obbligo di informativa devono obbligatoriamente fornirla nei casi in cui i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice sulla Privacy.

Anche in questi casi le regole dettate per la registrazione delle immagini vanno effettuate nel pieno rispetto del principio di proporzionalità. Il tempo massimo di conservazione dei dati è di 24 ore, salve ipotesi speciali di conservazione prolungata in relazione a peculiari esigenze tecniche, o particolare rischiosità dell'attività svolta dal titolare del trattamento. In ogni caso il tempo massimo non può superare la settimana.

Allo scadere del tempo previsto i sistemi di sorveglianza devono essere programmati anche per l'integrale cancellazione dei dati e dell'informazione. Qualora il sistema non preveda la cancellazione automatica questa deve essere fatta nel più breve tempo possibile.

Per il mancato rispetto dei tempi di conservazione delle immagini e della cancellazione è prevista una sanzione che va dagli € 3.000 agli € 180.000.

Per gli Enti comunali valgono regole speciali, ossia quando l'attività di videosorveglianza è diretta alla tutela e controllo del territorio, in questo caso la *"durata di conservazione dei dati è di sette giorni successivi alla rilevazione delle immagini e informazioni, salvo speciali esigenze di conservazione"*.

6.2 SETTORI SPECIFICI

Il provvedimento pone in risalto le regole per i settori specifici.

RAPPORTI DI LAVORO - Il primo limite è costituito dallo Statuto dei lavoratori, ove vige il divieto di utilizzo di sistemi di videosorveglianza a distanza per finalità di mero controllo.

Le organizzazioni sindacali aziendali rilasceranno le dovute autorizzazioni in base a esigenze organizzative e produttive, ovvero sicurezza sul lavoro. Il divieto è assoluto quando si tratti di spogliatoi, docce, armadietti e luoghi ricreativi.

Tali prescrizioni valgono sia all'interno dell'azienda sia all'esterno: ad esempio servizio taxi, servizi di linea per trasporto di cose e persone ovvero servizio di noleggio con conducente.

Il mancato rispetto delle disposizioni comporta sanzioni pecuniarie che vanno da € 30.000 a € 180.000.

Invece il controllo a distanza dei lavoratori per effettuare indagini sulle loro opinioni politiche integra la fattispecie di reato perseguibile sia con ammenda che ammonta dai 1.500,00 € ai 3.000,00 € nonché con l'arresto da 15 giorni ad 1 anno, peraltro il giudice a sua totale discrezione può aumentare l'ammenda fino a cinque volte, e ordinare la pubblicazione della sentenza stessa.

Rimane fermo il diritto di opporsi del lavoratore in caso di promozione dell'attività da parte dell'imprenditore con mezzi televisivi.

OSPEDALI E LUOGHI DI CURA - Stante la natura sensibile dei dati, le riprese devono essere limitate ai casi di stretta indispensabilità. Solo il personale medico-infermieristico può accedere alle immagini. Possono accedervi i familiari di ricoverati ove non possono recarsi personalmente (sala rianimazione). Il divieto è assoluto quando si tratta di estranei.

Il mancato rispetto delle regole comporta un'ammenda che va dagli € 30.000 agli € 180.000.

In caso di diffusione di dati che riguardano la salute, l'ammenda va dai 10.000 € ai 120.000 € nonché la reclusione da uno a tre anni se sussiste la finalità del profitto, ovvero recare ad altri un danno e se dal fatto deriva nocumento.

ISTITUTI SCOLASTICI - La tutela alla riservatezza impone il divieto di installazione di sistemi di videosorveglianza anche negli istituti scolastici, tenuto

conto che spesso tali contesti sono frequentati da minori. Le riprese andranno fatte nell'orario di chiusura delle scuole e circoscritte alle aree interessate.

L'eventuale installazione di sistemi di videosorveglianza è consentita per proteggere l'edificio ed i beni scolastici da atti vandalici.

Il divieto è assoluto anche in coincidenza di attività extrascolastiche che si svolgono all'interno della scuola.

L'ammenda va dagli € 30.000 agli € 180.000.

TRASPORTO PUBBLICO - Per l'installazione su mezzi pubblici e presso le fermate. L'angolo visuale deve essere circoscritto e le riprese vanno effettuate senza l'uso di zoom. I mezzi dotati di telecamere dovranno portare apposite indicazioni o contrassegni che diano conto della presenza dell'impianto di videosorveglianza.

L'assenza di informativa è punita con la sanzione che va dagli € 6.000 ai 36.000 €.

Il mancato rispetto delle altre regole produce di conseguenza l'applicazione della sanzione amministrativa tra gli € 30.000 a € 180.000.

WEBCAM O CAMERA ON-LINE - Anche l'utilizzo di webcam o camera on-line a scopi pubblicitari-turistici o esclusivamente pubblicitari deve avvenire con una modalità che renda non identificabili i soggetti ripresi, il rischio è che i dati finiscano in rete con la possibilità che vengano utilizzati da chiunque.

SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA - Si tratta di sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati o che consentono la fornitura di servizi di videosorveglianza.

Un soggetto pubblico può effettuare attività di videosorveglianza al solo scopo di svolgere funzioni istituzionali.

Le stesse amministrazioni, titolari di compiti in materia di pubblica sicurezza o prevenzione dei reati, possono installare telecamere ma devono motivare con esigenze effettive e proporzionali l'attività di prevenzione o repressione di pericoli concreti. Ad esempio è lecito controllare discariche di sostanze pericolose od eco piazzole, al fine di controllarne le modalità d'uso, la tipologia dei rifiuti scaricati e l'orario di deposito.

I privati, invece, possono trattare dati personali solo se vi è stato un consenso preventivo da parte dell’interessato.

Tuttavia, le telecamere possono essere installate senza il preventivo consenso degli interessati quando preservano da situazioni di pericolo, di sicurezza personale e tutela dei beni.

Ad oggi rimane scoperta l'ipotesi di videosorveglianza nelle aree condominiali, ambito non ancora ben definito dalla normativa.

Infatti non è chiaro se l'installazione di sistemi possa essere fatta in base alla sola volontà dei comproprietari o se rilevi anche la qualità di conduttori. Altro aspetto non chiaro riguarda il numero dei voti necessario per la deliberazione condominiale in materia: unanimità o maggioranza.

Il singolo condominio che voglia monitorare il proprio ingresso deve adottare opportune cautele, es. posizionamento con angolo visuale limitato ai soli spazi di propria pertinenza e nessuna ripresa di aree comuni o antistanti abitazioni di altri condomini.

Resta ferma la possibilità di installare videocitofoni al solo scopo di identificare i visitatori.

7. NOVITA' D.L. 6 DICEMBRE 2011 N. 201

Nella C.D. manovra Salva Italia il Governo ha emanato il Decreto-Legge 6 dicembre 2011 n. 2011, decreto che contiene importanti novità migliorative in materia di trattamento dei dati personali.

Il risultato della novità si palesa quando il soggetto di applicazione non è più il soggetto giuridico, che esce completamente dall'ambito di applicazione, ma rimane solo il soggetto fisico.

Non si sa se la scelta di estromettere le persone giuridiche sia stata consapevole o frutto di disattenzione derivante dalla fretta di applicare il Decreto.

Comunque sia il titolare ed il responsabile del trattamento continuano, limitatamente ai rapporti con le persone fisiche, ad essere obbligate ad eseguire tutti gli adempimenti imposti dal Codice della privacy.

8. PROTEZIONE DELLA PRIVACY NEI SOCIAL NETWORK

Dal punto di vista della tutela dei dati personali, questa tipologia di servizi consente un'agevole comunicazione di dati relativi agli utenti, e non solo tra questi, ma anche a soggetti terzi con le conseguenti lesioni della privacy.

In particolare il rischio è che una volta immessi i propri dati nel social network, gli utenti non riescano a gestirli in quanto possono venire a conoscenza delle informazioni anche soggetti non abilitati dall'utente. In questo caso la tutela è di scarsa effettività, infatti dopo la richiesta di cancellazione dei dati su richiesta dell'interessato non si ha la garanzia che soggetti terzi non possano ancora utilizzare i dati precedentemente acquisiti e copiati.

E' opportuno prestare molta attenzione alle informazioni che si decide di pubblicare, in quanto i dati stessi potrebbero riemergere in contesti e situazioni differenti. E' auspicabile evitare anche la diffusione di contatti personali.

Costituisce un illecito il trattamento d'uso delle immagini estratte dai social network per finalità giornalistiche, la cui corrispondenza tra i soggetti ritratti ed i protagonisti degli articoli di cronaca non è stata verificata.

E' obbligo dei fornitori vigilare sulle modalità con cui i dati dei propri utenti sono utilizzati dai terzi, i primi hanno la facoltà di decidere quali dati rendere pubblici e quali visualizzabili ai soli conoscenti.

In tal senso i fornitori devono predisporre dei meccanismi di consenso improntati all'*opt-out* per i dati non sensibili, od all'*opt-in* per i dati di natura sensibile contenuti nel profilo (es. opinioni politiche, orientamento sessuali ecc).

Deve essere inoltre garantita la possibilità di utilizzare pseudonimi, consigliando agli utenti l'esercizio di questa opzione.

Infine dato il rischio oggettivo per la riservatezza, gli standard di sicurezza adottati devono essere più stringenti; volti a garantire che soggetti terzi non possano scaricare o illecitamente sottrarre dei dati.

Nel caso di abbandono del social network da parte dell'utente i dati devono essere obbligatoriamente cancellati.

9. REGISTRO DELLE OPPOSIZIONI

Il D.P.R n. 178 del 7 settembre 2010 ha introdotto, in tema di privacy, un importante novità sul fronte del Telemarketing ovvero Marketing Telefonico.

La novità consiste nella tenuta da parte del Ministero dello Sviluppo Economico di un apposito registro, concepito a tutela di quei cittadini che non vogliono ricevere telefonate commerciali.

L'esigenza di creare il registro delle opposizioni nasce dalla necessità dei singoli cittadini che scelgono volontariamente di non ricevere telefonate con scopi commerciali.

Per esprimere il diniego a ricevere le comunicazioni commerciali il cittadino deve iscriversi al registro delle opposizioni. L'iscrizione può essere inoltrata con diverse modalità: raccomandata A/R, via fax, tramite posta elettronica; ad ogni modo, qualunque strumento venga adottato dal cittadino per la comunicazione del diniego, obbliga l'operatore ad eliminare quel nominativo dall'elenco in suo possesso.

Ciò significa che anche l'operatore è obbligato ad iscriversi al registro, comunicando la lista dei nominativi che intende contattare, pena l'irrogazione di sanzioni pecuniarie previste dal Codice della Privacy.

CAPITOLO SECONDO (copyright)

1. LEGGE SUL DIRITTO D'AUTORE NELL'ERA MULTIMEDIALE

Nell'era multimediale il diritto d'autore, la comunicazione delle opere dell'ingegno e la concreta possibilità che le stesse siano soggette a più soprusi è molto più semplice rispetto al passato. Tutto questo è reso possibile dalla velocità della rete, maggiore rispetto al cartaceo. Di conseguenza è quasi impossibile controllarne la circolazione, in tal modo le opere fruiscono nel luogo e nel momento scelto dall'utente, e copiare il contenuto di un’opera è molto più semplice. Tutto ciò dovrebbe far pensare che il diritto d'autore sia oramai difficilmente tutelabile, invece così non è infatti la normativa a disposizione della difesa delle opere è tutt’ora viva più che mai.

Uno degli aspetti tipici delle opere dell'ingegno è la vocazione "transnazionale", ovvero la fruibilità delle stesse al di là dei confini dello stato d'appartenenza dell'autore che le crea. Tanto per fare un esempio: in Italia posso liberamente scaricare un libro formato e-book di uno scrittore che si trova negli Stati Uniti.

Da ciò deriva che nel sistema delle fonti del diritto d'autore un ruolo di primaria importanza è svolto dai trattati Internazionali e dalle direttive Europee a cui i Paesi appartenenti all'Unione Europea devono aderire.

La normativa nazionale che attualmente regola la materia è la Legge 22 aprile 1941 n. 633 "Protezione dei diritto d'autore e di altri diritti connessi al suo esercizio, e successive modificazioni". Da qui in avanti la chiameremo (L.D.A).

Il Codice Civile prevede una regolamentazione generale della materia, la quale richiama in modo specifico la normativa speciale. Inoltre vi sono norme collegate alla tutela del diritto d'autore anche nel Codice Penale.

2. TUTELA DEL DIRITTO D'AUTORE

Secondo il Codice Civile e la L.D.A. sono tutela del diritto d'autore le opere dell'ingegno di carattere creativo che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro, e alla cinematografia, qualunque ne sia il modo o la forma di espressione.

Sono comprese nella protezione:

1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, sia in forma scritta che orale;

2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali costituenti di per sè opera originale;

3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti;

4) le opere della scultura, pittura arte e disegno, incisione, arti figurative e scenografia;

5) i disegni e le opere dell'architettura;

6) le opere dell'arte cinematografica, muta o sonora;

7) le opere fotografiche;

8) i programmi per elaborare in qualsiasi forma espressi purchè originali quale risultato di creazione intellettuale dell'autore;

9) le banche dati, intese come raccolte di opere, dati, o altri elementi indipendenti;
10) le opere del disegno industriale che presentino di per sè carattere creativo e valore artistico.

Il fatto che altre categorie di opere non siano espressamente comprese nell'elenco non significa che non possono esserci ulteriori tipologie che la legge tutela, infatti la giurisprudenza è sempre attiva in tale direzione.

Ad ogni modo, il primo requisito che la legge individua come indispensabile è il *"carattere creativo"*. La dottrina e la giurisprudenza riconducono il concetto di creatività ai requisiti di “originalità e novità”.

L’originalità è il risultato di un'attività dell'ingegno umano non banale; l'opera cioè deve rivelare un'elaborazione intellettuale risalenti alla personalità dell'autore.

La novità è da intendersi come novità di elementi essenziali e caratterizzanti tali da distinguere l'opera da quelle precedenti, cioè una novità in senso oggettivo.

A questa si contrappone una tesi secondo cui la novità non deve essere in senso assoluto, in quanto in qualsiasi opera è facilmente ravvisabile una traccia di precedenti creazioni altrui.

Pertanto si può dire che l'opera è dotata del carattere creativo quando reca l'impronta della personalità dell'autore riflettendone il modo personale di rappresentare ed esprimere fatti, idee e sentimenti, presentando caratteristiche individuali che rivelino l'apporto di un determinato autore.

LA FORMA ESPRESSIVA – L'attività creativa non può rimanere a livello di mero pensiero ma non occorre neanche che l'opera venga fissata su un supporto materiale, essendo sufficiente, per esempio per le opere letterarie, una comunicazione orale.

Semmai una mancata comunicazione formale, e il fatto che l'opera non sia stata fissata materialmente, determina un problema di prova circa la sua esistenza.

Al fine di determinare l'oggetto della protezione è utile ancora seguire una teoria del 900’ che opera una distinzione tra forma esterna, forma interna e contenuto dell'opera dell'ingegno.

Per forma esterna si intende l'opera come appare nella sua versione originaria, ovvero insieme di parole e frasi nelle opere letterarie; insieme di melodia, ritmo e armonia nell'opera musicale; la forma interna è la struttura espositiva dell'opera (organizzazione del discorso, scelta e sequenza degli argomenti nell'opera letteraria, i passaggi essenziali del discorso musicale).

Il contenuto è l'argomento trattato, le informazioni, i fatti, le idee, le opinioni e le teorie in quanto tali. Secondo tale teoria, la tutela ha per oggetto sia la forma esterna che interna, ma non il contenuto. Pertanto il principio che ne deriva è che la tutela riguarda la forma espressiva dell'opera e non il contenuto.

Non sono suscettibili di protezione né le semplici idee né forme espressive elementari non idonee a rappresentare fatti o sentimenti.

LE CREAZIONI UTILI **-** Il diritto d'autore tutela le "creazioni intellettuali" che suscitano reazioni emotive da parte del soggetto che ne viene a conoscenza. Nel tempo questa visione, che poteva benissimo adattarsi in altra epoca, ha subito un radicale stravolgimento, dettato soprattutto dall'ingresso nel mercato dell'informatica e dall'importanza di dare una tutela anche a questa fattispecie di opere. Infatti sono rientrate nella tutela del diritto d'autore tipologie di opere dove l'elemento emotivo è minore, se non assente. Tali creazioni sono costituite dai programmi per elaborare, le banche dati e il disegno industriale.

Le caratteristiche di tali opere sono:

1) finalizzate al raggiungimento di un risultato utile;

2) caratterizzate da aspetti in qualche modo predefiniti;

3) prevalenza della quantità di lavoro e del tempo impegnato nell'attività di creazione.

I programmi per elaborare contengono l'insieme delle istruzioni che vengono impartite all'elaboratore.

La tutela è limitata alla forma espressiva assimilata alla forma letteraria e non al contenuto. Le banche dati sono definite quali raccolte di opere, dati o altri elementi indipendenti, sistematicamente o organicamente disposti, accessibili grazie ai mezzi elettronici o in altro modo.

Vengono tutelate dal diritto d'autore se per la scelta o la disposizione del materiale costituiscono una "creazione intellettuale". In caso contrario è stata predisposta una tutela "sui generis" in favore di colui che per la loro costituzione effettui investimenti rilevanti.

Il disegno industriale consiste nella progettazione della forma di prodotti industriali destinati a soddisfare i bisogni della vita pratica.

Riguarda la creazione di una forma estetica pregevole del prodotto conforme alla sua funzione. Si tratta dell'unica opera dell'ingegno ove il legislatore richiede oltre al carattere creativo, anche il requisito del "valore artistico".

LE ELABORAZIONI CREATIVE **–** La L.D.A regola altresì il caso di creazione di un'opera dell'ingegno derivata da un'opera esistente, ove l'utilizzazione della seconda è subordinata all'autorizzazione del titolare dalla prima.

Sono protette quindi le traduzioni in un'altra lingua, le trasformazioni da un'altra forma letteraria od artistica, le modificazioni ed aggiunte che costituiscono un

rifacimento sostanziale dell'opera, adattamenti, riduzioni, compendi, variazioni non costituenti opera originale.

3. SOGGETTI E TUTELA DEL DIRITTO D'AUTORE

Con il termine "soggetti del diritto d'autore" si intendono i soggetti ai quali sono attribuiti i diritti d'autore e/o connessi.

Il codice civile e la L.D.A. stabiliscono che il titolo originario dell'acquisto del diritto d'autore è costituito dalla creazione dell'opera quale particolare espressione del lavoro intellettuale.

Il diritto in capo all'autore nasce dal solo fatto della creazione dell'opera senza che siano richiesti ulteriori adempimenti o formalità, quali ad esempio la pubblicazione dell'opera, il deposito o la registrazione. L'autore, ovvero la persona che ha creato l'opera, acquista tali diritti a titolo originario.

L'art. 8 L.D.A., stabilisce una presunzione legale di paternità dell'opera, che vale per le opere pubblicate: è reputato autore dell'opera chi in essa viene indicato come tale nelle forme d'uso o è annunciato come tale nella recitazione, esecuzione, rappresentazione e radiodiffusione dell'opera stessa.

Un aspetto importante da non sottovalutare e che spetta a chi contesta che l'opera non è stata creata da chi si è qualificato come autore, dare la prova della paternità.

La legge regola anche i casi delle opere frutto del contributo di più autori, prevedendo tre schemi di tutela:

3.1. OPERE IN COMUNIONE

Sono opere create con la collaborazione di più autori, il cui contributo è indistinguibile ed inscindibile, tra gli autori si costituisce una comunione per l'esercizio dei diritti di utilizzazione economica e morali, e sono regolate all’interno della L.D.A.

Le parti indivise si presumono di valore uguale, salvo la prova per iscritto di diverso accordo. Sono applicabili le disposizioni del codice che disciplinano la comunione. La difesa del diritto morale può comunque essere esercitata individualmente da ciascun co-autore. L'opera, senza l’accordo di tutti i co-autori, non può essere pubblicata se inedita, né può essere modificata o utilizzata in forma diversa da quella della prima pubblicazione.

3.2 OPERE COLLETTIVE

Sono costituite dalla riunione di opere o di parti di opere che hanno carattere di creazione autonoma, come risultato dalla scelta e del coordinamento a un determinato fine e sono regolate da una norma della L.D.A. La legge stessa le esemplifica nelle enciclopedie, nei dizionari, nelle antologie nelle riviste e nei giornali.

E' considerato autore chi organizza e dirige la creazione dell'opera stessa.

Il diritto di utilizzazione può spettare all'editore dell'opera stessa, mentre ai singoli collaboratori dell'opera collettiva è riservato il diritto di utilizzazione dell'opera stessa, salvo diverso accordo.

3.3 OPERE COMPOSTE

Sono le opere composte da contributi di generi artistici diversi, che sono distinguibili e utilizzabili separatamente, quali le opere liriche, le operette, le composizioni musicali con parole, le opere composte ecc.

Vi sono poi altre opere che non rientrano né nella definizione della L.D.A. né in altre leggi, come per esempio le "opere multimediali" che grazie alla tecnologia digitale riuniscono su uno stesso supporto opere di generi e di mezzi espressivi diversi (parola, musica, immagini) e le collegano e le amalgamano in modo da trattare e rappresentare un dato argomento.

Inoltre vi è il caso di opere create in esecuzione di "contratti di lavoro autonomo o subordinato".

Al contrario del rapporto di lavoro subordinato ove il datore acquista tutti i diritti e su tale punto dottrina e giurisprudenza concordano; nei rapporti di lavoro autonomo i diritti vanno riconosciuti al commissionario e non al committente. La L.D.A. prevede la possibilità di depositare l'opera presso alcuni registri che hanno natura di pubblicità notizia e non costitutiva del diritto.

4. CONTENUTO DELLA TUTELA DEL DIRITTO D'AUTORE

La L.D.A. individua due fasce indipendenti e separate di diritti attribuiti all'autore o al suo cessionario, "diritti di utilizzazione economica" e "diritti morali".

4.1 DIRITTI DI UTILIZZAZIONE ECONOMICA

I diritti di utilizzazione economica sono tipici delle opere dell’ingegno, sono generalmente riconosciute il diritto di pubblicazione, il diritto di riproduzione, il

diritto di trascrizione, il diritto di esecuzione, il diritto di rappresentazione e recitazione in pubblico, il diritto di diffusione, il diritto di distribuzione, il diritto di traduzione, elaborazione, pubblicazione in raccolta, il diritto di noleggiare e di dare in prestito.

Tali diritti regolati dalla L.D.A. sono trasmissibili, indipendenti l'uno dall'altro, con una durata limitata nel tempo e possono essere fatti valere "*erga omnes"* ovvero nei confronti di tutti.

La L.D.A. fa un elenco di tutta una serie di diritti non residuali, quali il diritto di tradurre, elaborare, modificare, trasformare, pubblicare in raccolta l'opera. Per questi diritti è necessario il consenso dell'autore. In generale vige il principio che ogni modifica del programma necessita del consenso espresso dell'autore. Il mancato rispetto delle norme a tutela di questi aspetti costituisce un ipotesi di plagio.

Sono però previste deroghe ai succitati principi, ovvero la presenza di un patto che escluda tali divieti. In tal caso le attività vietate devono essere necessarie per garantire la funzionalità del programma.

L'utilizzazione dei diritti ha una durata temporale limitata, pari ad anni 70 dalla morte dell'autore.

Una particolarità della L.D.A. è data dalla presenza di una previsione "quadro" dettata sempre dalla L.D.A. Si prevede che l'autore detenga il diritto esclusivo di utilizzare economicamente l'opera in ogni forma e modo, originale o derivato, nei limiti fissati da questa legge ed in particolare con l'esercizio dei diritti esclusivi indicati negli articoli seguenti.

La legge prevede inoltre singole fattispecie di durata a seconda delle diverse tipologie dell'opera. I termini finali si computano a decorrere dal 1 gennaio dell'anno successivo a quello in cui si verifica la morte dell'autore o altro evento considerato della norma.

4.2 I DIRITTI MORALI

L'autore conserva anche dopo la cessione, indipendente dall'aspetto economico, una serie di facoltà chiamati diritti morali.

Lo scopo del diritto morale è quello di proteggere la personalità dell'autore, che appunto si manifesta nella sua opera, purché questa rientri tra quelle che possono formare oggetto di tutela. L'autore può opporsi a qualsiasi utilizzazione dell'opera che avvenga con le modalità tali da pregiudicare la sua reputazione.

I diritti morali sono ritenuti inalienabili, irrinunciabili e imprescindibili al pari di tutti i diritti della personalità.

Tali diritti si scompongono in specifiche e determinate facoltà:

1) il diritto di rivendicare la paternità dell'opera e nel caso di opera anonima di rivelarne l'appartenenza;

2) il diritto di opporsi a deformazioni o modificazioni dell'opera e a ogni altro atto o danno che possano essere di pregiudizio all'onore o alla reputazione dell'opera stessa;

3) il diritto di ritiro dell'opera dal commercio per gravi ragioni morali.

4) il diritto di determinare il momento e i limiti di pubblicazione.

La legge non pone alcun termine alla durata dei diritti morali; alla morte dell'autore il diritto di paternità intellettuale e quello all'integrità dell'opera possono essere fatti valere dal coniuge, dai figli e così via.

5. ECCEZIONI AL DIRITTO D'AUTORE

La L.D.A. prevede un sistema di eccezioni e limitazioni ai diritti esclusivi dell'autore, in particolare il diritto di riproduzione e di comunicazione al pubblico. Tale sistema, contrapposto a quello anglosassone, trova la giustificazione della sua esistenza nella tutela di un interesse generale all'accesso alle idee, opinioni ecc. Troviamo eccezioni per pubblica utilità ed eccezioni per utilizzo personale, che valgono per i diritti di utilizzazione economica e non per quelli morali e sono di carattere eccezionale e di interpretazione molto restrittiva.

La costruzione dell'eccezione è sottoposta alle regole dettate dalle convenzioni internazionali che prevedono la subordinazione a tre condizioni:

1) limitazione ai soli casi speciali espressamente previsti dalla legge;

2) in modo da evitare contrasti con lo sfruttamento normale dell'opera;

3) in modo da non arrecare pregiudizio ingiustificato agli interessi legittimi del titolare.

6. TUTELA CIVILE

Oltre ai vari diritti riconosciuti la L.D.A contiene una seria di norme a tutela sia dei diritti di utilizzazione economica sia a difesa dei diritti morali.

Le azioni civili possono avere per oggetto:

1. l'accertamento della titolarità del diritto;

2. l'inibitoria dell'attività illegittima in violazione del diritto;

3. la rimozione o distruzione degli esemplari che costituiscono furti dell'illecito accertato;

4. l'interdizione dall'utilizzo dei fonogrammi;

5. il risarcimento del danno subito dal titolare del diritto leso;

La L.D.A. in particolare prevede:

1. le azioni di accertamento e interdizione, l'esibizione di documenti e la fornitura di informazioni, tra le quali quelle sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto;

2. la proibizione della rappresentazione o esecuzione;

3. le azioni di distruzione e di rimozione di esemplari di opere e apparecchi di riproduzione;

4. l'interdizione dell'utilizzo dei fonogrammi;

5. il risarcimento del danno;

Alcuni provvedimenti di natura cautelare contenuti nella L.D.A. sono rivolti ad assicurare le prove dell'avvenuta violazione e sono: la descrizione, l'accertamento, la perizia, il sequestro di ciò che si ritenga costituisce violazione del diritto di utilizzazione, l’inibitoria (con penalità di mora).

La L.D.A. prevede che il giudice possa ordinare che la sentenza venga pubblicata per la sola parte dispositiva in uno o più giornali.

La legittimazione all'azione spetta a colui che abbia la titolarità del diritto che si pretende violato: quindi l'autore o i suoi aventi causa.

Se l'autore ha ceduto il diritto di utilizzazione oggetto della violazione, può sempre intervenire a tutela dei suoi interessi nei giudizi promossi dal cessionario.

Legittimato ad agire è anche il possessore del diritto di utilizzazione o il rappresentante del titolare.

Un particolare tipo di legittimazione è inoltre attribuito alla S.I.A.E. (cfr. par. 10)

7. TUTELA PENALE

Alcuni articoli della L.D.A. disciplinano i reati contro il diritto d'autore, i quali sono perseguibili d'ufficio. La prescrizione, ovvero il termine ultimo per la presentazione della denuncia è quinquennale. Gli articoli contenuti nella L.D.A che disciplinano i reati contro il diritto d'autore sono:

1) protezione generale dei diritti di utilizzazione economica e morale;

2) protezione dei programmi per elaborare e delle banche dati;

3) abusiva duplicazione, riproduzione, trasmissione o diffusione e/o messa in commercio di opere dell'ingegno;

4) noleggio abusivo e abusiva fissazione su supporto della prestazioni artistiche;

5) equiparazione della vendita con patto di riscatto al noleggio;

6) distruzione del materiale sequestrato e confisca degli strumenti e dei materiali serviti o destinati a commettere i reati, nonché dei supporti;

7) abusiva decodificazione di trasmissioni audiovisive ad accesso condizionato;

8) diminuzione delle pene in caso di collaborazione con la giustizia.

8. MERCATO DELLE OPERE DIGITALI

Così come accade per il commercio delle opere ordinarie anche per i prodotti analogici si ravvisa la necessità di una tutela dell'opera stessa. In questo caso oggetto della cessione è il diritto di fruire/ usare quel determinato bene (testo, audio, video, software) secondo le modalità pattuite.

Sarà possibile fare riferimento in questo caso alla cessione dei diritti di godimento dell'opera.

Prima dell'avvento della digitalizzazione delle opere, un soggetto acquistava un libro ed entrava in possesso della copia fisica di quel dato volume, invece oggi quando un

soggetto acquista un e-book acquista un file, in sostanza la scelta di propendere per l'una o l'altra modalità d'acquisto pone il problema per la possibilità di copia dell'opera.

Le opere in forma digitale, infatti, possono essere copiate e duplicate a costo zero e senza che si verifichi un danno alla qualità del prodotto stesso.

L'interrogativo di diritto che sorge a questo punto è se un soggetto che scarica un formato digitale di un prodotto ha la possibilità di cederla, ad un prezzo più basso, e tenersi anche una copia o più copie.

L'analisi del tema è legato alla teoria del *first sale* (ossia prima vendita), la quale se applicata ai beni digitali solleva non poche problematiche in ragione della peculiarità di tali beni, idonei ad essere copiati e duplicati.

Il diritto di esaurimento della distribuzione trova conferma anche nella legge sul diritto d'autore, che afferma il diritto di quest'ultimo di effettuare ed autorizzare qualsiasi forma di distribuzione ma che tale diritto si esaurisce dopo la prima vendita legittima di una copia del programma.

Un caso famoso di *first sale* è stato quello tra Bobbs-Merrill, famoso editore Statunitense titolare dei diritti di un libro intitolato "The Castaway". All'interno della copertina c'era un avviso del prezzo minimo di vendita al dettaglio del libro, ovvero un dollaro. L'avviso riportava che ove il rivenditore avesse venduto il libro ad un prezzo inferiore sarebbe incorso nella violazione del *copy-right.* Nel corso del giudizio l'attore vantò la titolarità del diritto d'autore, ed il convenuto si difese affermando che qualunque fosse l'accordo tra l'editore e il grossista ciò non lo riguardava perché egli aveva concluso un contratto di vendita con il grossista e potevano essergli opposte esclusivamente le eccezioni relative a tale contratto e non quelle derivanti dai rapporti giuridici nascenti dal contratto invece intercorso tra l'editore ed il grossista. La Corte Suprema degli Stati Uniti investita della controversia, sottolineò come la legge sul *copyright,* concede al proprietario dei diritti d'autore il diritto di impedire che terzi possano fare copie di un'opera dell'ingegno, e come non conceda, invece, agli autori alcun diritto di controllare ed incidere sulla circolazione degli esemplari in possesso di soggetti privati dopo l'avvenuto acquisto.

Quindi chi acquista legittimamente una copia di un'opera dell'ingegno, potrà in un secondo momento, disporne nel modo che ritiene più opportuno e quindi potrà rivolgersi a terzi per un'eventuale vendita o anche prestarla, fermo il divieto di farne copie.

9.SIAE

La funzione istituzionale della SIAE consiste nell'attività di intermediazione per la gestione dei diritti d'autore. La SIAE concede le autorizzazioni per l'utilizzazione delle opere protette, riscuote i compensi per diritto d'autore e ripartisce i proventi che ne derivano. Svolge la propria attività in Italia servendosi dei propri uffici, e all'estero attraverso le Società d'autori straniere con le quali ha stipulato accordi di rappresentanza.

Non è obbligatorio aderire alla SIAE. L'adesione alla SIAE è libera e volontaria. L'autore può teoricamente decidere di curare direttamente i rapporti con gli utilizzatori per tutelare i propri diritti, ma di fatto l'intermediazione di una organizzazione specializzata e capillare è attualmente indispensabile.

In Italia l'attività di intermediazione è riservata dalla legge alla SIAE in via esclusiva. L'autore può comunque scegliere di aderire ad altre Società di autori di Paesi stranieri.

Dal momento in cui l'autore aderisce alla SIAE, si avvale della sua intermediazione per le utilizzazioni affidate alla sua tutela. Se interpellato direttamente, dovrà indirizzare alla SIAE gli utilizzatori per il rilascio delle autorizzazioni. L'autore non può concedere direttamente le autorizzazioni, non può rinunciare ai diritti e non può accordare riduzioni. Tutto ciò nell'interesse diretto dell'autore che, attraverso la gestione collettiva dei diritti, è garantito nei confronti degli utilizzatori, ai quali è assicurata la trasparenza di trattamento e la univocità di condizioni.

CAPITOLO TERZO (domini)

1. ICANN: STRUMENTO DI RISOLUZIONE DEI CONFLITTI

L'ICANN è un'associazione giuridica no profit presente a livello internazionale, la quale opera ha lo scopo specifico di regolamentare l'assegnazione e la gestione dei nomi a dominio. E' inoltre chiamata a dirimere i conflitti in materia attraverso un Registro e secondo un "Regolamento di assegnazione" (chiamato anche RAG).

L'ICANN al fine di essere presente a livello interno dei singoli Stati, ha delegato il compito di registrazione e controllo a distinte autorità Continentali che a loro volta lo hanno affidato ad autorità Nazionali.

Come abbiamo appena detto l'ICANN opera attraverso il Registro e provvede a garantire la funzionalità del servizio attraverso un'adeguata infrastruttura tecnica ed amministrativa, oltre a rendere operativo il dominio successivamente alla verifica. Un principio fondamentale che vige nel Regolamento di assegnazione (RAG) è il principio cronologico, in parole semplici "chi primo arriva prima si accomoda".

Un limite importante dal Regolamento è quello riguardante l'impossibilità di adottare dei nomi che per la loro peculiarità sono riservati, i C.D. TOP LEVEL DEMAINS (COUNTRY CODE).

2.ASSEGNAZIONE - SOSPENSIONE - REVOCA

REGOLAMENTO DI ASSEGNAZIONE - Attraverso il Registro si provvede a garantire la funzionalità del servizio dei nomi a dominio attraverso un'adeguata infrastruttura tecnica ed amministrativa. Il Registro rende attivo il servizio una volta che viene effettuato il controllo ispirandosi al principio cronologico del chi prima arriva prima è servito.

Con la richiesta di assegnazione colui che si registra si assume con apposita dichiarazione scritta (LAR) la responsabilità civile e penale del nome del dominio di cui chiede la registrazione.

A voler essere più precisi le modalità di registrazione e mantenimento dei nomi a dominio sono di due tipi: SINCRONA e ASINCRONA.

SINCRONA è basata sull'utilizzo del protocollo EPP e permette la registrazione in tempo reale.

ASINCRONA è basata sull'inoltro al registro del documento in forma cartacea.

La registrazione, fatta in entrambe le modalità, ha durata annuale. La procedura di riassegnazione può dirsi conclusa quando pervenuta al Registro la documentazione richiesta e verificata la sua validità, l'assegnazione dell'indirizzo elettronico viene caricato nel Database dei nomi assegnati (DBNA). Il dominio può essere oggetto di trasferimento ad altrui persona, in capo ad un soggetto, ovvero di successione a titolo universale o particolare, quindi è possibile il passaggio agli eredi, trasformazione societarie, cambio di denominazione, cessione del ramo d'azienda, fusione ed incorporazione.

VERIFICA **-** La verifica è un'attività di controllo volta ad accertare quanto dichiarato dal registrante e può essere effettuata:

A) chiedendo la documentazione al fine di accertarne la veridicità e la sussistenza dei requisiti soggettivi che hanno determinato la registrazione del nome e dominio stesso;

B) a campione, chiedendo al Registrer di inviare la documentazione. Questa richiesta deve essere fatta per iscritto;

C) in qualunque momento per motivi di necessità ed urgenza;

Nel caso in cui quanto dichiarato dal dichiarante non sia in linea con quanto comprovato dalla documentazione il Registro procederà alla revoca.

REVOCA **-** Per revoca si intende un atto o provvedimento da parte dell'autorità giudiziaria, ovvero da altra autorità competente (Es. Arbitro).

I nomi a dominio saranno revocati per 30 giorni, dopo di che saranno definitivamente cancellati.

La revoca d'ufficio è suddivisa in due tipologie distinte, e cioè:

MANCANZA DEI REQUISITI SOGGETTIVI **-** Si verifica quando l'interessato non ha più titolo al nome del domino, nel senso che ha perso le caratteristiche soggettive. In questo caso si attiverà una procedura apposita per cui i nomi passeranno da uno stato di revoca di 30 giorni, per poi passare allo stato di cancellazione.

MANCATA PRESENTAZIONE DELLA DOCUMENTAZIONE - Anche in caso di mancata presentazione della documentazione si attiverà una procedura simile, cioè i nomi passeranno nello stato di revoca e successivamente acquisteranno lo status di cancellazione.

3 . DOMINIO EUROPEO

Realizzato con vari Regolamenti CE, contengono le regole di naming per il dominio Europeo.

Qualunque soggetto può richiedere la registrazione. La richiesta oltre la dichiarazione d'impegno per il rispetto di tutte le condizioni di registrazione, deve contenere gli estremi identificativi del richiedente. Le dichiarazioni possono essere fornite anche in forma elettronica e sono:

A) dichiarazione di essere legittimato alla registrazione (ossia avere i requisiti minimi di soggettività giuridica);

B) dichiarazione (LAR) attraverso la quale si afferma che la richiesta è fatta in buona fede e non lede eventuali diritti di terzi;

C) dichiarazione a tutte le condizione di registrazione, comprese le disposizioni relative alla risoluzione stragiudiziale delle controversie;

I *Domain name* che vengono dichiarati dall'organo giurisdizionale di uno Stato membro come diffamatori, razzisti o contrari all'ordine pubblico sono bloccati dal Registro. Qualora a seguito di una procedura giudiziaria o stragiudiziale, venga dimostrato che la registrazione è lesiva dell'altrui diritto, la registrazione è revocabile.

Ad esempio nome a dominio identico ad un nome oggetto di un diritto riconosciuto (marchio), oppure contenente analogie tali da creare confusione ("typosquatting", creazione di nomi simili).

In presenza di tali situazioni, ai fini della revoca è necessario che il Titolare della registrazione non sia legittimato a far valere un proprio diritto sul nome in oggetto, ovvero in alternativa che la registrazione/utilizzazione sia avvenuta in mala fede.

I principali compiti di organizzazione e gestione sono affidati dal regolamento CE a due distinti e complementari organismi: il Registro ed i Conservatori del Registro.

Il primo svolge funzioni organizzative, amministrative e di gestione del dominio. Più specificamente si occupa di:

A) registrazione nomi a dominio;

B) gestione suddetti nomi e server;

C) manutenzione banche dati e dei servizi d'interrogazione delle stesse destinati al pubblico (who is).

Comunque tra le funzioni più importanti rimane il controllo di verificare le richieste di registrazione.

L'Ente aggiudicatario del ruolo di registro e l'EURid (European Registry of Internet Domain Names) il quale servizio consiste nel ricercare un nome a dominio e verificare se il nome ricercato è stato già registrato.

4. SOLUZIONE DELLE DISPUTE: STRADE PERCORRIBILI

La maggior parte delle controversie che ruotano attorno ai domini è generata dalla diffusione di fenomeni quali:

CYBERSQUATTING **-** Consiste nell'abusiva occupazione di porzioni del cyberspazio non occupate da legittimi proprietari. E' previsto dal Regolamento di assegnazione.

TYPOSQUATTING **-** Registrare nomi a dominio molto simili a marchi o nomi altrui, con la differenza di alcune lettere ed errore di digitazione (es. microsof***t*** - microsof***d***).

PORNOSQUATTING **-** Utilizzare il *domain name* per reindirizzare l'utente su un sito pornografico del tutto estraneo al titolare del nome e del marchio identico al dominio.

DOMAIN HOLDING **-** Consiste nella registrazione di un nome a dominio identico al nome o al marchio altrui senza che sia utilizzato.

L'utilizzazione di *domain name* corrispondenti al marchio o nome altrui è la prima causa di contestazione, che può essere risolta attraverso procedure differenti. Al termine della quale si avranno risultati totalmente differenti, cioè stessa questione risultati giudiziari o stragiudiziari differenti.

Il Regolamento dispute (RD) del 2009, contiene la disciplina per la risoluzione delle controversie relativamente ai domini italiani, strumento valido in alternativa alla via giudiziaria.

Le vie per la risoluzione delle controversie sono la procedura di ***rassegnazione*** e ***l'arbitrato.*** Inoltre accanto a queste due vie ve ne è una terza, cioè ***la composizione pacifica*** tramite trattativa di natura commerciale, è una sorta di contratto di vendita del diritto di utilizzazione del dominio.

4.1 PROCEDURA DI RIASSEGNAZIONE

E' una procedura elaborata nel 1999 dall'ICANN al fine di combattere il fenomeno dell'accaparramento abusivo del *domain name*.

I soggetti abilitati a prestare tali procedure sono i "Prestatori di servizio di risoluzione delle Dispute" (PSRD), rintracciabili anche su internet ove c'è un sito apposito.

Le domande vanno presentate all'apposito Registro, il quale dispone di un Regolamento. Il ricorso non ha natura giurisdizionale e quindi non esclude successivo ricorso all'autorità giudiziaria.

La procedura consiste nella verifica del titolo all'uso o alla disponibilità del dominio e la verifica che non sia registrato o mantenuto in mala fede.

Vige il principio *"tempus regit actum"*, cioè il regolamento si applica nella versione in vigore al momento del procedimento.

Il Regolamento dispute prevede che questa possa essere intentata da ogni persona fisica o giuridica avente i requisiti per la registrazione di un nome a dominio, previa opposizione all'assegnazione di chi ritiene aver subito un pregiudizio.

Qualora venisse sollevata, l'opposizione può essere considerata come un tentativo di conciliazione che potrebbe concludersi pacificamente.

Il Regolamento dispute, dispone che possono essere sottoposti a procedura di riassegnazione soltanto i nomi a dominio per i quali un terzo ricorrente affermi:

A) che il nome a dominio opposto sia identico o tale da indurre confusione rispetto ad un marchio o altro segno distintivo aziendale;

B) che l'attuale assegnatario non abbia diritto o titolo in relazione al nome o dominio opposto;

C) che il dominio sia stato registrato o venga usato in mala fede.

Se il Ricorrente prova congiuntamente le condizioni di cui alla lettera A e C e il Resistente non prova di aver diritto o titolo al dominio, quest'ultimo viene trasferito al Ricorrente.

Per quanto riguarda la lettera B il Resistente per avere diritto al domino deve provare:

A) che prima di avere notizia dell'opposizione in buona fede ha usato o si è preparato ad usare il nome a dominio, o un nome ad esso corrispondente, per offerta al pubblico di beni o servizi;

B) che è conosciuto come associazione o ente commerciale con il nome corrispondente al nome;

C) che del nome sta facendo un uso legittimo non commerciale, oppure commerciale senza sviare la clientela del Ricorrente o violare il marchio registrato.

Nel Regolamento dispute, sono elencate a titolo meramente esemplificativo circostanze ritenute di mala fede nell'uso o registrazione del nome a dominio, e cioè:

A) circostanze che inducono a ritenere che il dominio è stato registrato con lo scopo di cedere, concedere, in uso o altro modo trasferire il nome al ricorrente, titolare di un nome oggetto di un diritto riconosciuto dal diritto nazionale o comunitario o suo concorrente ed il mantenimento del nome a dominio;

B) circostanza per impedire al titolare del diritto ad un nome, marchio, denominazione anche geografica di utilizzare tale nome in concorrenza con quella del ricorrente;

C) circostanza per danneggiare gli affari di un concorrente;

D) attrarre, con lo scopo di trarne profitto, utenti di internet per ingenerare confusione;

E) il nome a dominio sia un nome proprio, di un ente pubblico, di un privato.

La procedura di riassegnazione è certamente più burocratizzata rispetto alla trattativa commerciale e si basa su un giudizio di mera interpretazione dei fatti e delle regole contrattuali, ovvero valuta le tre condizioni previste dal regolamento per procedere alla revoca o meno.

Ne consegue che con il ricorso, la magistratura ordinaria può adottare sia misure cautelari e/o condannare al risarcimento del danno subito.

Da manuale è il caso Armani, in questo caso il Tribunale ha dichiarato illegittimo l'uso da parte del titolare di un timbrificio nonostante l'avesse registrato prima dello stilista. Quest'ultimo ha vinto in base alle legge sui marchi (R.D. 21 giugno 1949, n. 929 - Art. 1). Nel caso di ricorso alla procedura di riassegnazione la decisione sarebbe stata diversa, comunque a favore del timbrificio, in base al principio "chi primo arriva, si accomoda".

4.2 ARBITRATO IRRITUALE

Vi è la possibilità di ricorrere presso l'arbitrato attraverso la clausola compromissoria, la quale si richiede al momento dell'assegnazione di un domain name, con apposita richiesta da inviare al Registro.

La parte che desidera dare avvio alla procedura arbitrale nomina un proprio arbitro fra quelli indicati nell'elenco degli arbitri, costituito presso il registro.

La suddetta nomina va comunicata al registro e alla controparte e contiene l'oggetto della domanda, le ragioni di fatto e di diritto, le proprie conclusioni, il proprio domicilio e l'indirizzo di posta elettronica. Inoltre contiene l'invito per la controparte alla nomina di un arbitro, sempre dello stesso elenco che dovrà avvenire entro 5 giorni lavorativi.

Gli arbitri di parte scelgono il presidente del Collegio entro 5 giorni lavorativi dalla nomina del secondo arbitro.

Il Collegio arbitrale si considera costituito a fare data dal giorno successivo all'accettazione dell'incarico da parte del collegio stesso.

Gli arbitri devono pronunciare la decisione entro 90 giorni dalla costituzione del Collegio arbitrale.

Si tratta di una procedura stragiudiziale di natura contrattuale ma a differenza della procedura di riassegnazione conferisce maggiori poteri al collegio decisionale. Infatti il Regolamento dispute dispone che il *"collegio può procedere a provvedimenti cautelari in caso di gravi motivi", e nel caso di istruttoria, il Collegio arbitrale può delegare gli atti di istruzione ad uno solo degli arbitri. Il Registro fornisce al Collegio tutte le informazione da esso richieste".*

La decisione arbitrale è pronunciata secondo equità ed essi si comportano "quali amichevoli compositori". Il lodo arbitrale è equiparabile a quello della magistratura ordinaria ed è inappellabile nel merito.

Tutte le decisioni sono pubbliche e sono conservate presso il Registro, vengono eseguite entro 5 giorni lavorativi dal ricevimento dalla comunicazione della decisione.

L'unico inconveniente potrebbe essere costituito dai costi della procedura, che sono un po’ più elevati rispetto a quelli previsti dalla "procedura di riassegnazione", si consideri peraltro che la giustizia ordinaria è ancora più lenta è più onerosa.

E' utile aggiungere che l'attività di accaparramento del domain name viene effettuata solitamente da soggetti che agiscono in ordinamenti giuridici diversi, per cui i costi elevati per il radicamento di un giudizio all'estero scoraggiano l'utente danneggiato.

CAPITOLO QUARTO (commercio elettronico)

1. INQUADRAMENTO GENERALE

L'espressione commercio elettronico indica lo scambio di beni e servizi attraverso una rete telematica.

Rientrano, più ampiamente nel termine commercio elettronico, le diverse attività che oggigiorno vengono sfruttate nella vendita e anche nella sola distribuzione di contenuti digitali, trasferimento elettronico dei fondi, servizi di promozione dei prodotti ecc.

L'imponente diffusione delle imprese virtuali ha notevolmente ampliato e migliorato il panorama delle vendite via internet facendo sempre di più crescere il fenomeno appunto denominato e-business ovvero e-commerce.

Sotto il profilo soggettivo, possono individuarsi diverse categorie di e-commerce, e cioè: il professionista, il consumatore e il soggetto pubblico.

Per entrambe le formule lo scambio della volontà e la conseguente formazione dell'accordo avviene e si ottiene su internet. E' proprio questo uno dei punti centrali del capitolo che andremo ad analizzare onde fornire al lettore, sia che si tratti di un'impresa sia che si tratti di un soggetto fisico, una diagnosi delle precauzioni da tener presente qualora faccia uso dello strumento del e-commerce.

2. NEGOZIO GIURIDICO TELEMATICO

Le transazioni on-line hanno in comune l'autodeterminazione di ogni singolo soggetto il quale decide in ordine ai propri interessi, in questo caso si parla di autonomia privata o autonomia negoziale.

Ed infatti il negozio giuridico è comprensivo di ogni manifestazione di autonomia privata. Le attività in rete possono essere sfruttate attraverso manifestazioni unilaterali di volontà, ad es. "remissione del debito", "dichiarazione di disdetta" oppure "dichiarazione di recesso".

3. NATURA CONTRATTUALE DELLE TRANSAZIONI E-COMMERCE

Tra gli aspetti più importanti delle fattispecie contrattuali che si realizzano sul web, il primo elemento da considerare è *l'assenza di fisicità e simultaneità*. I contraenti infatti non sono uno di fronte all'altro, di conseguenza l'unica modalità di manifestare la volontà di concludere il contratto è quella a distanza.

C'è però un aspetto importante da considerare circa gli aspetti contenutistici, e cioè il contenuto del contratto è predisposto dal soggetto economicamente più forte, quello che ha più interessi nella partita, ossia il fornitore di beni e servizi. Quest'aspetto pone non pochi problemi in ordine alle due posizioni contrattuali.

4. CONTRATTAZIONE A DISTANZA E DISCIPLINA

In questa categoria è possibile comprendere la figura del contratto telematico, il quale si caratterizza per essere concluso tra soggetti non presenti mediante l'utilizzo della rete internet. Le differenti tipologie di comunicazione telematiche, ad esempio mail o il web, rientrano nella definizione di comunicazione a distanza.

La caratteristica della distanza viene a mancare qualora anche un solo elemento che forma la volontà dei soggetti si svolga con la presenza fisica e simultanea di fornitore e consumatore. Oppure anche quando è fisicamente presente il bene oggetto dell'accordo contrattuale.

Con riferimento alla categoria dei contratti a distanza, le varie normative succedutesi nel tempo hanno avuto l'obiettivo di disporre a favore del soggetto debole-consumatore una serie di rimedi processuali volti a sancire il diritto all'equilibrio informativo, con riferimento alla fase negoziale, e a garantire un diritto al ripensamento sulla convenienza della scelta compiuta.

5.OBBLIGHI INFORMATIVI

Per quanto concerne il profilo informativo, il fornitore di beni e servizi deve in fase precontrattuale fornire al consumatore suo interlocutore, una serie di informazioni che devono risultare chiare e comprensibili, assumendo come parametro quello del consumatore sprovveduto.

In particolare, il fornitore deve comunicare la propria identità e qualora il contratto preveda un pagamento anticipato, dovrà indicare anche il suo indennizzo. Inoltre devono essere comunicate le caratteristiche del bene o del servizio offerto, il prezzo dello stesso, comprese eventuali spese di consegna e le modalità di esecuzione contrattuale previste.

Inoltre devono essere comunicate eventuali costi aggiuntivi derivanti dalla tecnica di comunicazione utilizzata, la durata dell'offerta, la durata minima del contratto in caso di esecuzione continuata o periodica e le relative modalità di recesso.

Nelle contrattazioni in rete l'obbligo di informativa nei consumatori è inderogabile mentre per i professionisti è derogabile tramite accordo tra le parti.

Nell'e-commerce vi è l'obbligo per il prestatore di indicare i riferimenti che permettono di contattarlo rapidamente e di comunicare con lui direttamente ed efficacemente, fra i quali l'indirizzo di posta elettronica.

Non è obbligatorio l'inserimento del numero di telefono.

Inoltre vi è l'obbligo di fornire in modo chiaro, comprensibile ed inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario del servizio, tutte le informazioni inerenti altre varie fasi tecniche della conclusione del contratto; quali le modalità di correzione dei dati inseriti, le modalità di archiviazione e di accesso al contratto, l'eventuale predisposizione di strumenti di composizione delle controversie o di adesione a codici di condotta.

Se il destinatario del servizio è un consumatore i succitati obblighi sono inderogabili, in caso contrario l'obbligo può essere derogato con un semplice patto tra le parti.

6. IL DIRITTO DI RECESSO

La normativa prevede che sia lo stesso fornitore a dover informare il consumatore sui suoi diritti, con particolare riguardo a quello di recesso, indicandone sempre in modo intellegibile le modalità ed i tempi di esercizio, nonché le modalità di presentazione dei reclami, le informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti.

Al momento della conclusione dell'accordo contrattuale, tutte le informazioni devono essere messe a disposizione del consumatore su un supporto duraturo. Nel caso di operazioni via internet, viene riconosciuta la possibilità di inserire nella pagina

contenente l'offerta, le informazioni generiche a riguardo, oltre ai termini e alle modalità di esercizio del diritto di recesso, rinviando ad altra pagina web collegata all'offerta, per avere tutte le informazioni dettagliate.

Il diritto di recesso del consumatore è attribuito dalla legge al solo consumatore in quanto parte debole, affinché questi possa esercitarlo senza dover ottenere il consenso del professionista. La ragione del diritto al recesso sta nella possibilità del consumatore di avere il tempo per valutare adeguatamente le condizioni del contratto sottoscritto.

Un aspetto molto importante è quello in cui il recesso si riferisce ad un contratto di durata o ad esecuzione immediata. Nel primo caso si può recedere dalla durata del contratto ma non per le prestazioni già eseguite od in corso di esecuzione. Nel secondo caso si può recedere fino a quando il contratto non avrà avuto un principio di esecuzione.

Il consumatore può recedere dal contratto a distanza entro 10 giorni lavorativi, termine che decorre nel caso di beni dal giorno del ricevimento da parte del consumatore, e nei servizi dal giorno della conclusione del contratto.

RECESSO PER I PRODOTTI SOFTWARE E AUDIOVISIVO - Un altro aspetto molto importante riguarda il diritto di recesso il quale viene escluso quando si tratta di prodotti audiovisivi o di un software e nello specifico quando la confezione sia stata aperta. La ragione di quest'esclusione sta nel fatto che si tratta di beni utilizzabili in un arco di tempo inferiore al diritto di recesso stesso. Un prodotto audiovisivo potrebbe infatti essere visionato e poi restituito, oppure il software addirittura può essere installato e poi restituito.

In caso di recesso viene peraltro stabilito un limite per le spese accessorie a carico del consumatore e cioè il consumatore in caso di recesso dovrà sostenere solo le spese dirette di restituzione del bene al mittente.

FORO DI COMPETENZA – Il foro di competenza risulta di difficile determinazione per quanto riguarda i contratti telematici, si ritiene esso sia determinato in relazione alla residenza o al domicilio del consumatore.

7.ELENCO DETTAGLIATO DEI DIRITTI DEI CONSUMATORI

Una tematica sempre più interessante dal punto di vista normativo concerne i contratti conclusi tra *professionista e consumatore*, questo interesse è dovuto sia per l'elevato numero di transazioni sia perché sono caratterizzati dalla debolezza di uno dei due soggetti coinvolti nelle operazioni commerciali, in questo caso il soggetto più debole è il consumatore finale, ossia colui che è interessato all'acquisto.

Proprio per questo motivo è necessaria una disciplina specifica di tutela dell*'e-commerce* e limitazioni dei poteri del professionista, affinché a quest'ultimo venga limitata la sua forza contrattuale e la possibilità di sfruttare la propria posizione a proprio vantaggio.

Ed infatti l'imprenditore interessato a prestare un servizio, come la vendita, deve adottare tutti gli accorgimenti necessari affinché venga realizzato un accordo contrattuale corretto.

Abbiamo già anticipato la posizione del destinatario del servizio, o meglio del consumatore, cioè una posizione di debolezza. A quest'ultimo il legislatore ha riconosciuto una serie di regole necessarie a correggere tale squilibrio, regole le quali si rivolgono con particolare attenzione alle condizioni generali di contratto e alla stipulazione di formulari o modulari. In quest'ultimo caso è sempre la parte più forte, ossia il professionista che provvede alla stesura, motivo per cui tali contratti si considerano efficaci nei confronti dell'altra parte *"se al momento della conclusione del contratto chi le ha accettate le ha riconosciute o avrebbe dovuto riconoscerle usando l'ordinaria diligenza";*

"Qualora il regolamento contenga condizioni vessatorie, (condizioni sfavorevoli al consumatore) non sono efficaci se non sono specificamente approvate per iscritto".

La normativa di riferimento è contenuta nel codice del consumo ove sono elencati tutti i diritti dei consumatori, e cioè*:*

a) tutela della salute;

b) alla sicurezza e alla qualità dei prodotti e dei servizi;

c) ad una adeguata informazione e ad una corretta pubblicità;

d) all'educazione al consumo;

e) alla correttezza, trasparenza ed equità nei rapporti contrattuali;

f) promozione e sviluppo associazionismo libero, volontario e democratico tra i consumatori e utenti;

g) erogazione di servizi pubblici secondo standard di qualità ed efficienza

8. SPECIFICA DISCIPLINA DEL E-COMMERCE

Al fine di garantire un certo grado di trasparenza del servizio, al venditore che eroghi uno o più servizi vengono imposti particolari adempimenti, nello specifico si tratta di quelle che vengono definite *"informazioni generali obbligatorie"*.

Infatti, il venditore deve rendere facilmente accessibili in modo diretto e permanente, ai destinatari del servizio le informazioni di carattere identificativo, è cioè:

a) il nome, la denominazione o la ragione sociale;

b) il domicilio o la sede legale;

c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente con lo stesso, compreso l'indirizzo di posta elettronica;

d) il numero di iscrizione al repertorio delle attività economiche, REA, o registro delle imprese;

e) gli elementi di individuazione, nonché gli estremi della competente autorità di vigilanza qualora un'attività sia soggetta a concessione, licenza od autorizzazione;

Per quanto riguarda le professioni regolamentate:

1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione;

2) il titolo professionale e lo stato membro in cui è stato rilasciato;

3) il riferimento alle norme professionali e agli eventuali codici di condotta vigenti nello stato membro di stabilimento e le modalità di consultazione dei medesimi;

f) il numero della partita IVA o altro numero di identificazione considerato equivalente nello stato membro se il prestatore svolge attività soggetta ad imposta;

g) identificazione in modo chiaro ed equivocabile dei prezzi e delle tariffe dei diversi servizi;

h) indicazioni delle attività consentite al consumatore e al destinatario del servizio.

Gli obblighi informativi riguardano anche le comunicazioni commerciali ed in particolare quelle "non sollecitate" (Spamming). La normativa a proposito è molto chiara e sancisce che *"devono in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al loro ricevimento per il futuro"*.

PRIMA DELL'INOLTRO **-** L'attenzione che il legislatore rivolge alla figura del consumatore è molto attenta, infatti prevede che il venditore deve fornire in modo chiaro, comprensibile e inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario di un bene o di un servizio, una serie di informazioni riguardanti i principali aspetti del contratto stipulato.

Nello specifico, le notizie che la normativa prevede debbano essere comunicate al consumatore sono:

a) le varie fasi tecniche da seguire per la conclusione del contratto;

b) il modo in cui il contratto concluso sarà archiviato e le relative modalità d'accesso;

c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dati prima di inoltrare l'ordine all'operatore;

d) eventuali codici di condotta cui aderisce e come accedervi via telematica;

e) le lingue a disposizione per concludere il contratto oltre all'italiano;

f) l'indicazione degli strumenti di composizione delle controversie;

Se la modalità di conclusione del contratto è esclusivamente lo scambio di messaggi di posta elettronica, il proponente non è obbligato alle prescrizioni normative imposte.

Per il mancato rispetto di tutti gli obblighi fin qui richiamati è prevista, salvo che il fatto costituisca reato, sanzione amministrativa da € 103,00 ad € 10.000,00. Nei casi di gravità o recidiva i limiti minimi e massimi sono raddoppiati.

9. CLAUSOLE VESSATORIE

Le clausole vessatorie sono disciplinate e contenute nel codice civile, il resto è stato inserito nel codice del consumo dove troviamo le regole per limitare l'autonomia privata del professionista, al fine di evitare abusi a danno del consumatore, ricordandoci che quest'ultimo nel codice del consumo rimane sempre e comunque la parte più debole del rapporto.

In base alla normativa *"sono vessatorie, quelle clausole che una volta inserite provocano uno squilibrio di condizioni a sfavore del consumatore"*.

La norma contempla venti clausole ritenute abusive, la presunzione non è assoluta e può essere superata del professionista che dovrà dimostrare che l'assetto contrattuale complessivo è tale da annullare ogni squilibrio a scapito del consumatore.

Nello specifico sono:

a) Informazioni generali obbligatorie;

b) Obblighi di informazione per la comunicazione commerciale;

c) Comunicazione commerciale non sollecitata;

d) Uso delle comunicazioni commerciali nelle professioni regolamentate;

e) Informazioni dirette alla conclusione del contratto;

Inoltre in base al Codice Consumo, "si presumono vessatorie fino a prova contrarie le seguenti clausole":

a) escludere, o limitare la responsabilità del professionista in caso di morte o danno alla persona del consumatore;

b) limitare le azioni o i diritti del consumatore nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale;

c) escludere o limitare l'opportunità da parte di un consumatore della compensazione di un debito nei confronti del professionista con un credito vantato nei confronti di questi;

d) prevedere un impegno definitivo del consumatore mentre l'esecuzione della prestazione del professionista è subordinata ad una condizione dipendente dalla sua volontà;

e) consentire al professionista di trattenere una somma versata dal consumatore qualora quest'ultimo non concluda il contratto o recede da esso, senza prevedere il diritto del consumatore di esigere dal professionista il doppio della somma se quest'ultimo non concluda il contratto;

f) imporre al consumatore, in caso di inadempimento o ritardo, il pagamento di una somma a titolo di risarcimento o una penale eccessivi;

g) riconoscere solo al professionista e non al consumatore il diritto di recedere dal contratto;

h) consentire al professionista di recedere da contratti a tempo indeterminato senza un ragionevole preavviso, tranne per una giusta causa;

i) stabilire un termine eccessivamente anticipato rispetto alla scadenza del contratto per comunicare la disdetta;

l) prevedere l'estensione dell'adesione del consumatore a clausole che non ha avuto possibilità di conoscere;

m) consentire al professionista di modificare unilateralmente le clausole del contratto, o le caratteristiche del prodotto, senza un giustificato motivo;

n) stabilire che il prezzo dei beni e servizi sia determinato al momento della consegna o della prestazione;

o) consentire al professionista di aumentare il prezzo senza che il consumatore possa recedere dal contratto se il prezzo è eccessivamente elevato rispetto a quello convenuto;

p) riservare al professionista il potere di accertare la conformità del bene venduto o conferire il diritto esclusivo d'interpretare una clausola qualsiasi del contratto;

q) limitare la responsabilità del professionista derivante da contratti stipulati in suo nome dai suoi mandatari;

r) limitare o escludere l'opponibilità dell'eccezione dell'inadempimento da parte del consumatore;

Si presumono invece vessatorie, le clausole che, pure essendo state oggetto di trattativa individuale abbiano per oggetto o per l'effetto di:

a) escludere o limitare la responsabilità del professionista in caso di morte o danno alla persona del consumatore, risultante da un fatto o da un'omissione del professionista;

b) escludere o limitare le azioni del consumatore nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di inadempimento inesatto da parte del professionista;

c) prevedere l'adesione del consumatore come estesa a clausole che non ha avuto, di fatto, la possibilità di conoscere prima della conclusione del contratto.

Il sistema anche in questo caso tende una mano alla figura del consumatore, infatti è previsto che le clausole ritenute vessatorie non sono nulle quando operano a vantaggio del consumatore, il contratto rimane efficace per il resto. E' inoltre rilevabile d'ufficio, quindi non comporta che l'impugnazione deve avvenire da parte del consumatore.

10. CONCLUSIONE DEL CONTRATTO VIRTUALE

Il nostro ordinamento è ispirato al principio della libertà della forma, e prevede che la forma scritta debba prevalere, a pena di nullità, soltanto nei casi tassativamente indicati dallo stesso codice.

Tra le forme libere si annoverano dichiarazioni (scambi di volontà) che si servono della posta elettronica o che si realizzano attraverso il web.

E' di certa applicazione anche il contenuto delle norme in base al quale il contratto è costituito dall'incontro di due o più volontà e si conclude *"nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte"*. A ciò si aggiunga anche il principio della *"presunzione di conoscenza"*.

11. L'ACCORDO TELEMATICO

L'accordo telematico può formarsi tramite scambio di proposta e accettazione tramite internet.

Se il contratto prevede la forma scritta è possibile attraverso l'invio telematico del regolamento negoziale all'interno di un documento siglato con firma digitale.

Una seconda tipologia è quella dell'accettazione della proposta fatta tramite vetrina virtuale, attraverso la pressione del tasto negoziale virtuale (o point and click). Il prestatore allestisce la vetrina on-line ove è precisato il contenuto dell'accordo negoziale (comportamento concludente).

La conclusione point and click è valida per tutti i contratti a forma libera ed è esclusa quando la legge richiede la forma scritta a pena di nullità.

Il codice civile ammette anche un altro schema e cioè " *il contratto è concluso nel tempo e nel luogo in cui ha avuto l'esecuzione"*. Un esempio pratico riguarda i contratti “Business to consumer”, dove le transazioni aventi ad oggetto beni o servizi sono normalmente correlate al pagamento tramite carta di credito. La digitalizzazione del codice ha il valore per la validità del contratto.

Vi è peraltro in questo caso una tutela a favore del consumatore. Infatti un D.Lgs. prevede che gli Istituti di emissione sono tenuti ad accreditare al Consumatore i pagamenti per i quali dimostri che c'è stato un uso fraudolento della propria carta di credito, inoltre le somme accreditate al legittimo proprietario vengono addebitate al Fornitore, il quale è peraltro del tutto estraneo alla vicenda.

Il Fornitore non ha strumenti a disposizione per dimostrare la buna fede e per liberarsi dall'obbligo della restituzione delle somme suddette, neppure quando ha adottato tutte le cautele necessarie e possibili.

In verità quanto sopra rappresenta uno squilibrio tra la posizione del consumatore e quella del fornitore dove quest’ultimo rimane senza una garanzia.

12. REVOCA DELLA PROPOSTA

La proposta può essere revocata finché il contratto non sia concluso, e anche l'accettazione può essere revocata purché la revoca giunga a conoscenza del proponente prima dell'accettazione.

La revoca della proposta e dell'accettazione sono atti che producono effetto nel momento in cui giungono all'indirizzo del destinatario, seppure attenuati dalla previsione di presunzione di conoscenza.

In base a quanto contenuto nel Codice civile, il contratto è concluso nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte; di conseguenza la revoca della proposta sarebbe possibile fino a quando il proponente non abbia notizia dell'accettazione.

13. TEMPO E LUOGO DI CONCLUSIONE DEL CONTRATTO VIRTUALE

La determinazione del tempo e del luogo di stipulazione del contratto è essenziale per diversi motivi. Un motivo tra tutti è quello necessario per determinare i profili attinenti alla giurisdizione e alla competenza.

Secondo la disciplina generale dei contratti, l'accordo si conclude nel momento e nel luogo in cui si trovano le parti all'atto dell'incontro delle rispettive dichiarazioni negoziali; in particolare, relativamente allo scambio di proposta e accettazione via web, le indicazioni di luogo e di tempo potrebbero essere:

a) contratti conclusi via mail: nel tempo e nel luogo in cui, attraverso l'operazione di download il proponente ha notizia dell'accettazione da parte del destinatario del messaggio;

b) contratto concluso mediante pressione del tasto negoziale (point and click): trattandosi di accettazione per comportamento concludente nel tempo e nel luogo in cui il proponente ha notizia dell'accettazione da parte dell'oblato;

c) contratto concluso mediante il pagamento della prestazione pecuniaria: si tratta di ipotesi di conclusione mediante inizio dell'esecuzione; i negozi conclusi attraverso tale modalità si considerano conclusi nel tempo e nel luogo di inizio dell'esecuzione del contratto;

d) contratto concluso mediante offerta al pubblico: si considera concluso nel tempo e nel luogo in cui la dichiarazione negoziale di un qualsiasi destinatario dell'offerta al pubblico perviene all'indirizzo del proponente;

e) contratto concluso mediante invito a proporre: si considerano conclusi, nel momento e nel luogo in cui l'utente (proponente) riceve notizia dell'accettazione da parte del titolare del sito (oblato) contenente l'invito a proporre.

Quanto al tempo della stipulazione del contratto telematico, non sembra si presentino particolari difficoltà. Vi sono a chiarimento le norme del codice in base al quale il contratto si conclude quando chi ha fatto la proposta viene a conoscenza dell'accettazione dell'altra parte. Il momento della stipulazione coincide, quindi, con quello in cui la dichiarazione giunge all'indirizzo virtuale del destinatario, a prescindere dalla conoscenza che egli ne abbia avuto e sempre che non dimostri di essere stato senza sua colpa nell'impossibilità di averne notizia.

14.REGISTRO DELLE OPPOSIZIONI

Il Registro delle Opposizioni è una novità che rafforza la tutela del cittadino ed è in linea con quanto disposto dal Codice della privacy. Infatti, chiunque, non desideri ricevere comunicazioni di natura commerciali potrà iscriversi al "Registro delle opposizioni" (cosiddetta Robinson List).

In base alla Robinson List qualunque operatore economico che desidera avviare operazioni di telemarketing "mediante l'impiego del telefono e della posta cartacea", deve preventivamente registrarsi al Sistema, comunicando i recapiti di tutti coloro ai quali intende inviare le comunicazioni commerciali. In seguito il gestore setaccerà il Registro e lo restituirà depurato da tutti i nominativi presenti che hanno manifestato l'opposizione. *(www.registrodelleopposizioni.it).*

15. TRASMISSIONE DI ATTI E DOCUMENTI CON POSTA CERTIFICATA

Il Codice delle amministrazioni digitali, visto la necessità della ricevuta di consegna, dispone che le pubbliche amministrazioni utilizzino soltanto la posta elettronica certificata (PEC). L'importanza della PEC sta appunto nella prova dell'avvenuta ricezione.

La funzione assolta dalla PEC è simile a quella della raccomandata ordinaria tradizionale anche nel suo valore legale.

Chiaramente conferisce veridicità circa la ricezione del messaggio ma non del suo contenuto, ove in questo caso è necessaria la firma digitale.

16. REQUISITO DELLA FORMA NEI CONTRATTI ELETTRONICI

Un importante passaggio da considerare per la validità è il requisito dalla forma del contratto.

La forma non è altro che la modalità attraverso cui la volontà delle parti ed il consenso del contratto vengono manifestati all'esterno. La disciplina generale dei contratti prevede la libertà di forma, nel senso che l'accordo delle parti può essere esteriorizzato con qualsiasi mezzo ritenuto idoneo a realizzare le rispettive volontà negoziali.

In base a tali principi gli utenti si assumono l'auto-responsabilità dei rischi connessi alla conclusione di contratti telematici.

La forma scritta è sempre preferibile in quanto è più facile risalirne dal punto di vista probatorio. In altri termini il contratto è pienamente valido ad efficace, ma la sua esistenza non potrà essere provata e fatta valere in giudizio con mezzi diversi dalla forma scritta, se non attraverso il giuramento o la confessione.

c) firma elettronica qualificata: è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

d) firma digitale: è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata. Consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di verificare la provenienza e l'integrità di un documento informatico o un insieme di documenti informatici.

17.IL VALORE GIURIDICO DELLE FIRME ELETTRONICHE

Il valore giuridico che può attribuirsi al documento elettronico nel nostro ordinamento, munito o meno di firma digitale, è contenuto nel Codice di Amministrazione Digitale (CAD).

Sul piano sostanziale lo stesso CAD dispone che il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, soddisfa il requisito della firma scritta previsto dal codice civile.

18.LA PUBBLICITA' COMMERCIALE ON LINE

Il concetto di pubblicità generalmente inteso, quale pubblicità commerciale può benissimo essere applicato al mondo di internet, seppure con caratteristiche diverse.

Come abbiamo detto Internet rappresenta uno strumento essenziale del commercio Internazionale, proprio grazie alla sua capacità di diffondere informazioni senza limiti geografici ed in tempo reale. Questo vale anche per la pubblicità on-line, divenuta uno strumento che consente rispetto al modello tradizionale la compravendita immediata di prodotti.

Altra caratteristica fondamentale è che al contrario della pubblicità tradizionale, dove il consumatore subisce passivamente il messaggio con le tecniche comunicative tradizionali, la pubblicità on-line consente all'utente di essere parte attiva, la cui caratteristica è basata sulla interattività ed attitudine informativa volta a catturare l'utente finale.

Inoltre, è interessante notare dal punto di vista dell'impresa, che ogni messaggio promozionale o contenuto editoriale viene erogato attraverso un server che registra le richieste degli utenti, con conseguente tracciabilità del percorso del messaggio e quindi dell'utente.

Allo stato attuale, la diffusione delle comunicazioni commerciali on-line avviene attraverso una serie di modalità.

Innanzitutto vi è il *banner*, un'inserzione solitamente rettangolare, che appare dai siti web e sollecita la curiosità del consumatore portandolo ad aprire il messaggio.

Dai banner sono poi derivate altre modalità quali *l'interstitial*, uno *spot* che appare automaticamente in seguito alla richiesta di una pagina *web* ed è programmato per durare il tempo necessario al *download*.

Accanto a queste pubblicità tabellari, ve ne sono altre come la *sponsorship*, ossia l'abbinamento di un marchio ad un evento.

Una pratica assai diffusa è quella dell'invio del messaggio pubblicitario tramite e-mail. Inoltre c'è la *newsletter*, ove con uscite quotidiane o settimanali vengono trattati argomenti e la *mailing list*, ossia una sorta di *forum* dove vengono trattati argomenti tramite posta elettronica.

Il carattere transnazionale del sistema e la possibilità di diffusione del messaggio senza confini geografici si riverberano anche sulla pubblicità on-line. In questo senso è preferibile fare riferimento alle norme del diritto Internazionale privato, volte a dirimere il conflitto fra norme peculiari a singoli ordinamenti.

Sul piano comunitario troviamo il Regolamento (CE), il quale prevede una cooperazione fra le autorità pubbliche all'uopo designate da ciascun Stato membro al fine di tutelare i consumatori. In questo caso ove una pratica commerciale lesiva dei consumatori italiani origini un altro S.M., l'Autorità Garante della Concorrenza e del Mercato (AGCOM) può richiedere al corrispondente soggetto pubblico competente di svolgere indagini volte ad accertare la violazione, nonché l'applicazione di eventuali misure coercitive.

Sul piano del diritto interno, all'assenza di una vera e propria disciplina specifica della pubblicità on-line si ovvia estendendo le norme sulla pubblicità commerciale, in generale contenute nelle direttive CE ed in alcuni D.Lgs. sulla pubblicità ingannevole nei rapporti fra professionisti e nel Codice del consumo riguardo alle pratiche commerciali scorrette nei confronti dei consumatori.

PRATICHE SCORRETTE **-** Uno dei D.lgs. ha introdotto la figura delle *pratiche commerciali scorrette*; mentre l'altro ha dettato una disciplina in materia di *pubblicità ingannevole e comparativa illecita nei rapporti fra professionisti.*

Per i professionisti è prevista una tutela dalla pubblicità ingannevole e comparativa illecita nei loro reciproci rapporti commerciali.

C'è una definizione ben precisa di pratica commerciale scorretta che è opportuno richiamare. Per pratica commerciale scorretta deve intendersi "qualsiasi azione o omissione, condotta o dichiarazione, comunicazione commerciale ivi compresa la pubblicità e la commercializzazione del prodotto, posta in essere dal professionista, in relazione alla promozione, vendita o fornitura di un prodotto ai consumatori che possa alterare sensibilmente la capacità del consumatore di prendere una decisione consapevole, inducendolo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".

L'Agcm può, in base ai succitati decreti ed in caso di pubblicità ingannevole e comparativa nonché per le pratiche commerciali scorrette avviare procedimenti anche d'ufficio, essendo dotata di poteri istruttori e sanzionatori, sono infatti previste sanzioni che vanno da 1.000 ai 100.000 Euro.

Ulteriore disciplina a difesa del Consumatore è riscontrabile in disposizioni penalistiche, come ad es. i messaggi pubblicitari che abbiano un contenuto lesivo delle convinzioni morali, civile, religiose o della dignità della persona, che possono causare un abuso della credibilità popolare o trarre in inganno il consumatore.

Altra tutela è prevista dal codice civile che vieta la concorrenza sleale, e comunque ritiene illecita la pubblicità menzognera, denigratoria, superlativa, imitativa e quella che possa ingenerare confusione con altri prodotti o servizi.

CAPITOLO QUINTO (reati informatici)

1. VIOLENZA SULLE COSE (Art. 392 C.P.)

"Chiunque, al fine di esercitare un diritto preteso, potendo ricorrere al giudice, si fa arbitrariamente ragione da se medesimo, mediante violenza sulle cose è punito a querela .... omissis ....".

Il comportamento sopra descritto è riportato in seno all'art. 392 c.p. caratterizzato da connotati di autotutela del soggetto agente, il quale ritiene di essere titolare di un diritto.

Può trattarsi di un diritto obiettivamente esistente o soltanto supposto, purché sussistano elementi di fatto che facciano apparire come verosimile l'esistenza dello stesso. E' necessario che esista la possibilità di ricorso al giudice sia in termini fattuali che giuridici.

Nel primo caso è necessario che il soggetto non si trovi in una condizione tale da essere impossibilitato a fare ricorso all'autorità giudiziaria. Nel secondo caso è necessario che il diritto preteso sia suscettibile di effettiva realizzazione giudiziale.

Capita spesso che un sistema informatico, ovvero i programmi in esso contenuti, vengano aggrediti con finalità di autodifesa laddove potrebbe astrattamente ottenersi tutela con l'esercizio di un'azione giudiziaria.

Un esempio che può chiarire le idee sull'istituto in questione è ravvisabile nel caso, che capita non di rado, di un programmatore incaricato di sviluppare un software, il quale abbia fondata ragione di temere che il committente potrebbe non pagare la prestazione. Il programmatore scoraggiato dalle lungaggini della giustizia, potrebbe inserire un virus nel programma stesso. Questo è un caso richiamato appunto dall'art. 392 terzo comma c.p.

Quindi un software si considera alterato ogniqualvolta ne è stata modificata l'essenza attraverso una manipolazione totale o parziale del codice sorgente.

2. ATTENTATO A IMPIANTI DI PUBBLICA UTILITA' (Art. 420 c.p.)

"Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità è punito, salvo che il fatto costituisca reato più grave, con la reclusione da uno a quattro anni".

Il bene giuridico tutelato è l'ordine pubblico che si ritiene violato al verificarsi del fatto. Si tratta di un delitto di attentato o a consumazione anticipata, cioè un delitto che si consuma non appena viene posta in essere l'azione diretta a danneggiare o distruggere, e prescinde dal fatto che si sia effettivamente causato il danno o la distruzione.

L'attuale società ne fa larghissimo uso per svolgere attività di pubblica utilità.

C'è da segnalare che l'art. 420 c.p. subisce una scomposizione con la L. 547/1993 art. 2, ove la norma prevede da questo momento due distinte ipotesi, rispettivamente:

1 concernenti fatti diretti a danneggiare o distruggere impianti di pubblica utilità

2 sistemi informativi o telematici di pubblica utilità (primo comma), ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti (secondo comma).

Fu, altresì, inserita al terzo comma un'ipotesi aggravata se dagli stessi fatti fosse derivata *"la distruzione o il danneggiamento dell'impianto o del sistema dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema".*

Con L'art. 6 della L. n. 48/2008 il testo della disposizione in esame ha subito un'ulteriore modifica, attualmente si fa esclusivo riferimento a "impianti di pubblica utilità" senza altri riferimenti ad altre tipologie, ed è scomparso il riferimento ai dati (informazioni e programmi). Con l'unica definizione di "impianto" il legislatore ha voluto riferirsi anche ai sistemi informatici e telematici nonché ai dati in essi contenuti.

3. TUTELA PENALE DEI DOCUMENTI INFORMATICI (Art. 491 bis c.p.)

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private"

L'art. 491 bis ha esteso la fattispecie del falso materiale e ideologico ai documenti informatici (pubblici o privati) aventi efficacia probatoria. E' stata così superata la netta distinzione tra documento cartaceo e documento informatico, con ampliamento di quest'ultimo in prospettiva di difesa.

Il documento deve essere dotato di efficacia probatoria, ciò impone un richiamo alle disposizioni dettate dal Codice dell'amministrazione digitale.

Attualmente ai fini penali, la nozione di documento informatico è contenuta nel Codice dell'amministrazione digitale, con conseguente applicabilità anche alle disposizioni che ne regolano l'efficacia probatoria.

Infatti il D.Lgs. n. 82/2005 (art. 1 lettera p) definisce il documento informatico quale *"rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti".*

Da ciò se ne ricava che il documento elettronico che non è sottoscritto con una firma elettronica (art. 1 lettera q), non può avere alcuna efficacia probatoria ma può al limite, a discrezione del giudice, soddisfare il requisito legale della forma scritta (art. 20 comma 1 bis);

Quando il documento non è firmato da una firma elettronica semplice (cioè non qualificata) può non avere efficacia probatoria. Il giudice dovrà tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità e non modificabilità del documento informatico. Infine il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata ha l'efficacia prevista dall'art. 2702 c.c. (scrittura privata, quindi fa piena prova fino a querela di falso, se colui contro il quale è prodotto ne riconosce la sottoscrizione).

E' importante rilevare che nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche; ricorre la prima quando vi è divergenza tra l'autore apparente e l'autore reale del documento o quando questi sia stato alterato successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contiene dichiarazioni non veritiere o non fedelmente riportate.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo in forma elettronica altrui.

Non sembrano trovare applicazione le norme che puniscono le falsità in fogli firmati in bianco (art. 486, 487, 488 c.p.).

Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Tra i reati richiamati dall'art. 491 c.p. sono punibili a querela della persona offesa la falsità in scrittura privata (art. 485 c.p.), l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

Rimane però la difficoltà di sanzionare penalmente ipotesi di falsificazione del documento informatico. A causa della suddetta differenza, tale disposizione, non protegge alcune situazioni riconducibili in astratto al tema del falso; in quanto il falso su di un documento cartaceo risulta attraverso gli strumenti tecnici visibile con maggiore o minore facilità a seconda di chi falsifica.

Il falso su di una firma digitale falsa, al contrario, non esiste per lo meno nel senso tradizionale. Tutt'al più potrà sorgere un utilizzo abusivo del dispositivo di firma. L'utilizzo della smart card sottratta può integrare il reato di ricettazione o truffa, e nel caso si tratti di sottrazione dello strumento elettronico nei confronti della pubblica amministrazione può integrarsi il reato di truffa aggravata (art. 640 c.p.).

4. FALSE DICHIARAZIONI SU FIRMA ELETTRONICA (Art. 495 bis c.p.)

"Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno".

Il richiamo da fare in questo caso è rivolto al ruolo del certificatore. L'art. 1, comma I L. g, D.Lgs n. 82/2005 definisce il certificatore *"il soggetto che presta servizi di certificazioni delle firme elettroniche o che fornisce altri servizi connessi con queste ultime"*. Il Codice dell'amministrazione digitale contempla varie categorie di certificatori: semplice, qualificato e accreditato.

L'art. 495 bis non fa differenze tra questi, per cui si presume si possa applicare alle condotte consumate nei confronti di qualsiasi tipo di certificatore.

Rimane aperto un problema, ossia quello della possibile classificazione dei certificatori, in particolare quelli qualificati o accreditati nel novero dei pubblici ufficiali. In tal caso potrebbe ipotizzarsi un concorso con il reato di *"false dichiarazioni sull'identità o su qualità personali proprie o di altri"*, ove è prevista una sanzione ben più grave (reclusione da 1 a 5 anni).

5. ACCESSO ABUSIVO A UN SISTEMA INFORMATICO O TELEMATICO (Art. 615 ter c.p.)

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi mantiene contro la volontà espressa o tacita da chi ha diritto di escluderlo, è punito con la reclusione fino a tre anni".

La pena è da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso di poteri o con violazione di doveri inerenti alla funzione o al servizio, o da chi esercita abitualmente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati;

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica, alla sanità o alla protezione civile, la pena è rispettivamente della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso del primo comma il delitto è punibile a querela, negli altri casi d'ufficio.

L'art. 615 ter c.p., disciplina il reato di *"accesso abusivo ad un sistema informatico o telematico"*, inserito nei delitti contro la persona, Capo III *"dei delitti contro la libertà individuale"*, Sez. IV *"dei delitti contro la inviolabilità del domicilio"*.

L'obiettivo della norma è di tutelare il sistema informatico inteso come vera e propria estensione del domicilio dell'individuo.

Si tratta di un reato comune che può essere commesso da chiunque.

La norma prevede due condotte, in alternativa;

a) introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza;

b) il mantenimento all'interno del medesimo sistema contro la volontà espressa o tacita;

La prima ipotesi punisce il mero accesso in presenza di misure di sicurezza, cioè misure tecniche, informatiche, organizzative e procedurali volte a escludere o impedire l'ingresso al sistema.

La seconda ipotesi si riferisce, invece, al mantenimento nel sistema informatico nonostante il titolare abbia comunicato, in maniera espressa o tacita, la volontà di esclusione.

Nella definizione di sistema informatico rientra il sistema informatico hardware (elementi fisici costituenti l'unità di elaborazione e tutte le periferiche di input e output) e il software (programmi per elaboratore di base e applicativi); il sistema telematico è composto da una serie di componenti informatici collegati tra di loro mediante una rete telematica.

La Cassazione ha stabilito che per sistema informatico e telematico debba intendersi il *"complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione anche parziale di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di codificazione e decodificazione - dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati di dati, cioè di compilazione diverse, e dalla elaborazione automatica di tali dati, in modo da ingenerare informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente"*.

Per quanto concerne le misure di sicurezza, l'orientamento che è stato accolto anche dalla giurisprudenza conclude che basta una qualunque misura di protezione, anche banale e facilmente aggirabile, in quanto la presenza della misura di sicurezza sarebbe da intendersi non tanto quale misura di protezione effettiva del sistema ma, piuttosto, come elemento in grado di rendere esplicita e non equivoca la volontà di escludere l'accesso da parte di chiunque non abbia il consenso del titolare.

L'elemento psicologico è il dolo generico e il sistema informatico/telematico per poter subire un accesso abusivo deve essere protetto da una qualsivoglia forma di sicurezza (protezione, nome utente e password o protezione fisica).

Il sistema informatico è contemplato nella fattispecie come domicilio, appunto domicilio informatico. Per essere riservato è necessario che il titolare adotti una misura di sicurezza. Da ciò ne consegue che nel caso in cui il sistema informatico non sia protetto in alcun modo non può sussistere il reato di accesso abusivo.

6. ACCESSO E DIFFUSIONE ABUSIVA DI CODICI D'ACCESSO (Art. 615 quater c.p.)

Chiunque, al fine di procurare a se o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione da uno a due anni e al pagamento della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater".

La disposizione in esame configura un reato di pericolo, volto ad anticipare la tutela rispetto all'evento dannoso.

La disposizione punisce la detenzione non autorizzata di codici di accesso (password, PIN, smart card) e anche la loro diffusione illecita a terzi non autorizzati. Costituisce reato anche la mera diffusione di istruzioni tecniche su come eludere o ottenere i suddetti codici.

Non è sufficiente la detenzione o la diffusione illecita di codici ma è necessario che da tale detenzione o diffusione ne derivi un profitto per sé o per altri, ovvero un danno a terzi (cosiddetto dolo specifico).

Rientra in tale fattispecie anche la clonazione di un cellulare.

Il secondo comma prevede sanzioni più severe e cioè la reclusione da uno a due anni e multa da dieci a venti milioni di euro, se il fatto è posto a danno "di un sistema informatico o telematico utilizzato dallo Stato o altro ente pubblico (art. 617 quater, quarto comma, n. 1, c.p.) o è commesso *"da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso di poteri o violazioni di poteri inerenti la finzione o al*

servizio, ovvero con abuso di qualità di operatore del sistema". (art. 617 quater, quarto comma, n. 2 c.p.).

7. DANNEGGIAMENTO DEL SISTEMA INFORMATICO (Art. 615 quinquies c.p.)

"Chiunque allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione totale o parziale o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.369".

Si tratta in sostanza della diffusione di tutti i programmi che rientrano sotto la categoria di virus informatici ma anche della diffusione di componenti hardware (smart card pen drive) in grado di danneggiare sistemi informatici e/o telematici.

I virus sono costituiti da porzioni di codice sorgente che si diffondono all'interno di altri programmi (completi), in modo tale da essere eseguiti ogni volta che il file infetto viene eseguito.

La diffusione può avvenire sia tramite supporti (DVD, CD-ROM), sia attraverso le reti telematiche.

La norma mira sia a reprimere la diffusione di questi codici maligni e la mera detenzione dei codici stessi. Inoltre la norma reprime chiunque li procuri, diffonda, comunichi, consegni e metta a disposizione programmi, apparecchiature o dispositivi.

L'elemento soggettivo è circoscritto al dolo specifico, ossia è punibile soltanto se commesso "allo scopo di danneggiare illecitamente un sistema informatico o telematico e le informazioni, i dati o i programmi in esso contenuti".

8. DANNEGGIAMENTO DI INFORMAZIONI E DATI (Art. 635 bis c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella altera o sopprime informazioni, dati o programmi informatici altrui è punito a querela dalla persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena prevede la reclusione da uno a quattro anni e si procede d'ufficio".

L'art. 635 bis c.p., prevede la procedibilità a querela di parte e non più d'ufficio se non nei casi aggravati dalla violenza o minaccia, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Successivamente è stato introdotto anche l'art. 635 ter c.p. *(Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)* e l'art. 635 quinquies c.p. *(Danneggiamento di sistemi informatici i telematici di pubblica utilità).*

Queste due nuove fattispecie sono state introdotte nella sezione dedicata ai reati contro il patrimonio così da tenere separati i beni giuridici protetti: da una parte informazioni, dati e programmi nell'art. 635 ter e dall'altra parte i sistemi informatici o telematici nell'art. 635 quinquies.

Entrambe le fattispecie presentano l'aggravante dell'effettivo danneggiamento, con una pena edittale che parte da un minimo di tre anni fino ad un massimo di otto anni.

9. FRODE INFORMATICA

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto, con qualsiasi modalità su 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 è punito con la reclusione da sei a tre anni e con la multa da euro 51 a euro 1.032".

"La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma

dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema".

"Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

L' Art. 640 ter c.p. punisce l'illecito arricchimento conseguito attraverso l'impiego fraudolento di un sistema informatico.

Potrebbe definirsi, vista la condotta, come una truffa realizzata a mezzo del computer; ma visto che l'ingiusto profitto e l'altrui danno sono diretta conseguenza dell'inganno teso al computer e non alla persona risulta difficile ipotizzare il reato di truffa.

Nella truffa il soggetto agente dirige la sua condotta direttamente verso l'uomo in moda da indurlo in errore; nella frode informatica la condotta si dirige verso il computer, facendo leva sul rapporto di fiducia che l'uomo ha nei riguardi dell'elaboratore.

Inoltre per realizzarsi il reato di truffa manca un elemento indispensabile e cioè la collaborazione prestata dal soggetto passivo in conseguenza dell'inganno.

L'uomo si avvale del computer per ricevere un aiuto nello svolgimento delle sue attività e così instaura un rapporto fiduciario con la macchina; proprio questo rapporto è alla base della frode informatica, e infatti il delitto in esame può essere individuato come reato di aggressione al patrimonio realizzato mediante *"sfruttamento dello stato di soggezione che lega il soggetto passivo al suo sfruttamento di lavoro"*.

Ai sensi della norma in esame è importante chiarire il significato di sistema informatico. Sono tali quegli apparati che forniscono beni o servizi gestiti da un elaboratore; rientrano in tale definizione le fotocopiatrici, i telefoni cellulari, i distributori automatici di banconote etc. Non sono compresi invece, anche se la definizione è assai ampia, i congegni elettronici di apertura e chiusura, i quali hanno esclusiva funzione di protezione in sostituzione delle tradizionali serrature.

10. VIOLAZIONE DELLA CORRISPONDENZA E DELITTI DI INTERCETTAZIONE

Le nuove forme di comunicazione (invio di e-mail o in generale scambio di informazioni in rete) impongono nuove forme di tutela della corrispondenza e più in generale della libertà di comunicazione.

Così un primo intervento ha riguardato l'art. 616 c.p. che tutela la corrispondenza informatica e telematica ovvero ogni comunicazione a distanza.

L'art. 617 quater è finalizzato all'impedimento dell'intercettazione fraudolenta che si configura quando si prende conoscenza delle comunicazioni altrui in maniera occulta e senza esserne legittimato. Il dolo è generico e si procede a querela della persona offesa. Un esempio sono i fuori onda intercettati e diffusi, nei programmi televisivi e trasmissioni televisive interne.

L'Art. 617 quinquies c.p. sanziona la semplice predisposizione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Ad esempio qualora si installi su uno sportello bancomat, in sostituzione del pannello originario, un'apparecchiatura composta da un superficie plastificata con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat.

L'Art. 617 sexies c.p. punisce il comportamento di chi falsifica, altera o sopprime il contenuto delle comunicazioni informatiche o telematiche. Il reato si consuma a seguito di una delle condotte descritte purché ci sia il dolo specifico e qualora ne faccia un uso illegittimo.

11. PEDOPORNOGRAFIA *(Legge 3 Agosto 1998 N. 269 e Legge 6 Febbraio 2006 N. 38)*

Mentre in passato non vi era una vera è propria tutela, tranne sporadici riferimenti normativi, la vera novità arriva con la L. 3 agosto 1998 n. 269 nata per contrastare le cosiddette nuove forme di riduzione in schiavitù (sfruttamento della prostituzione, pornografia, turismo sessuale in danno ai minori). Le novelle (art. 600 bis, 600 ter, 600, quater e art. 600 quinquies c.p.) furono inserite immediatamente dopo l'art. 600 c.p. (dedicato al reato di riduzione in schiavitù).

Successivamente il legislatore intervenne nuovamente con la L. n. 38/2006, per una tutela sempre maggiore del minore.

Furono apportate modifiche all'art. 600 ter e 600 quater c.p. e fu introdotto il reato di pornografia virtuale (art. 600 quater bis c.p.)

Un segnale chiaro di rinforzare la tutela per il minore si ebbe attraverso l'istituzione del centro Nazionale per il contrasto della pedopornografica sulla rete internet;

Vengono inseriti obblighi specifici per i fornitori di servizi e società dell'informazione resi attraverso le reti (internet service provider).

12. PEDOPORNOGRAFIA MINORILE (Art. 600 TER C.P.)

"Chiunque, con qualsiasi mezzo distribuisce, divulga, diffonde o pubblicizza il materiale pornografico, ovvero distribuisce o divulga notizie finalizzate allo sfruttamento sessuale è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.

Chiunque, offre o cede ad altri, il materiali pornografico, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.

La pena è aumentata in misura non eccedente ai terzi ove il materiale sia di ingente quantità".

L'intento della norma è chiaro e sta nel punire i soggetti che producono o esibiscono materiale pornografico con qualsiasi mezzo, sia cartaceo, sia tramite supporti digitali che producono e che commercializzano materiale pornografico.

Per materiale pornografico deve intendersi materiale osceno, offensivo del comune senso del pudore; inoltre deve trattarsi di materiale raffigurante un soggetto minore di 18 anni.

Per quanto affermato non rientra nella definizione di materiale pedopornografico ogni immagine che ritrae minori senza indumenti. Ad es. il bimbo nudo al quale viene scattata la foto in spiaggia dal genitore. Potrebbe acquistare valenza pedopornografica se cadendo nelle mani sbagliate venisse utilizzata al fine eccitare la sessualità altrui.

Anche la Cassazione sembra preferire tale soluzione. La legge n. 38/2006 ne ha esteso l'ambito di applicabilità considerando la semplice utilizzazione di minori e non più sfruttamento.