Problemi di Diritto dell'Informatica (Appello 11 maggio pomeriggio)

Diritto Contrattuale

Caratteristiche Fondamentali del contratto:

a) *Accordo*: caratteristica tipica del contratto è infatti l'essere un negozio giuridico bi o pluri-laterale. Il suo perfezionamento è dato infatti dall'accordo di almeno due parti.
b) *Patrimonialità*: il contratto è un negozio giuridico di natura patrimoniale in quanto ha ad oggetto rapporti suscettibili di valutazione economica

Elementi costitutivi del contratto (che non possono mancare):
Accordo: ovvero il reciproco consenso delle parti in merito alla vicenda contrattuale. Con il termine "consenso" si intende una in equivoca manifestazione di volontà diretta a porre in essere il contratto stesso, manifestazione anche non scritta e anche tacita.
Causa: cioè la funzione pratica del contratto, l'interesse socio – economico (e quindi non soggettivo) che il contratto mira a soddisfare
Oggetto: cioè il contenuto del contratto, ciò che le parti stabiliscono, programmano in merito al rapporto. Per oggetto del contratto si può anche intendere, tuttavia, la realtà materiale o giuridica su cui cadono gli effetti del contratto stesso
Forma: è il mezzo tramite il quale si manifesta la volontà contrattuale

Norma imperativa: si intende l'apposizione da parte dell'ordinamento giuridico di norme inderogabili dalla volontà delle parti.
Ordine pubblico: si intende l'insieme dei principi di struttura politica ed economica della società, immanenti nell'ordinamento giuridico vigente

Contratto: è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale (Art. 1321 Codice Civile, senza patrimonio non può esistere il contratto). L'incidenza di due attività preliminari porta alla fine alla stesura di un contratto. La con sensualità di intenti definisce un contratto. Esso nasce dall'incidenza di bisogni e offerte di due parti.

La forma scritta serve solo per alcuni contratti: Testamento – Acquisto/Vendita immobiliare – Donazione Normalmente il contratto non è formale a volta determinate forme di contratto si perfezionano verbalmente; ad esempio la garanzia fideiussoria è verbale (non serve formalizzarla)

La modifica verbale di cose scritte nel contratto (tipo slittamento dei termini) non occorre inoltre sia nuovamente scritta (basta una prova testimoniale). Se invece si vuole modificare l'oggetto del contratto che è scritto allora la prova testimoniale dopo la modifica verbale non basta (poiché entra in gioco la parte di codice civile delle prove).

Il contratto non è statico, può essere modificato o estinto. L'importante è che sia un rapporto Giuridico Patrimoniale.

Nell'ambito del contratto vige il principio dell':

Autonomia Contrattuale: le parti possono liberamente determinare il contenuto del contratto nei limiti imposti dalla legge (il contenuto del contratto non può violare la legge o andare contro l'ordine pubblico). Le parti possono anche concludere contratti Atipici purché siano diretti a realizzare interessi meritevoli di tutela per l'ordi

namento giuridico(norme imperative, ordine pubblico).

I contratti si dividono in:

- *Nominati* (Art. 1321): sono così chiamati poiché hanno un nome e sono regolamentati da articoli appositi nel Codice Civile. Si possono fare solo piccole modifiche
    - *Tipici*
        - Vendita (Art. 1470)
        - Appalto (Art. 1665): una parte realizza un opera o un servizio per una seconda parte pagante (lo sviluppo di software e i service sono alla fine degli appalti)
        - Comodato (Art. 1803)
- *Innominati* (Art. 1322): sono quei contratti che non hanno corrispettivo all'interno del codice civile (si ricordi che il CC è degli anni 40', all'epoca certe forme di contratto non esistevano), ma che ci si può ricondurre a un contratto del codice

- *Tipici*
  - Leasing
  - Body Rental
  - Licenza d'uso Software (funziona come un contratto di locazione o noleggio, in caso di interpretazione il giudice va a vedere la locazione come contratto di riferimento)
- *Atipici:* non si trovano nel codice
  - Joint Venture (è atipico poiché è molto vario a seconda dell'ambiente)

I contratti posso essere *Misti*: risultano dalla combinazione di contratti tipici, dalla convergenza di numerose forme di contratto. All'interno di un contratto misto vi è sempre una figura contrattuale predominante alla quale si fa riferimento in materia di legislazione (anche per la regolamentazione giuridica). A fianco al contratto principale vi sono una serie di:

Contratti Accessori: sono contratti che pur avendo una loro specifica causa sono in stretta dipendenza da un contratto principale. I contratti accessori sono particolarmente importanti nell'ottica di un sistema contrattuale.

Sviluppo di un Contratto Consensuale: avviene in vari modi:

1. Verbalmente
2. Con sottoscrizione (firma) di apposito contratto
3. Con un offerta accettata espressamente
4. Con un offerta accettata implicitamente
5. Aderendo a un offerta di controparte
6. Modificando un offerta di controparte

Una forma scritta non può essere modificata con un contratto consensuale in quanto la forma scritta è una prova. Meglio specificare il tutto nei documenti tecnici.

Analisi della fase precontrattuale: è la prima fase di stipulazione di un contratto, rilevante poiché:

A. Definisce caratteristiche e prestazioni del prodotto
   - Obbligo del fornitore di informare
   - Obbligo del cliente di informarsi
B. Può condurre al perfezionamento del contratto anche in assenza di forma scritta
   - La forma scritta del contratto è necessaria solo per alcuni specifici contratti (compravendita immobiliare, appalto, testamento)
C. Può avere particolari ripercussioni in caso di interruzione delle trattative (ad esempio se è stato sostenuto un costo per la predisposizione dell'offerta)
   - L'interruzione delle trattative (soprattutto nel caso sopra) non deve avvenire in mala fede (Art. 1337). Trattative e responsabilità precontrattuale. Le parti nello svolgimento delle trattative e nella formazione del contratto devono comportarsi secondo buona fede
D. Può condizionare la stipulazione del successivo contratto

Accordo Quadro: è un vero e proprio contratto, è vincolante, poiché raggruppa una serie di intese, in assenza di una riserva (ossia se non c'è scritto che ha solo valore informativo). Con essi le parti evidenziano tutti gli aspetti dell'intesa che desiderano porre in essere al fine di offrire una visione piena e di costituire un punto di riferimento per identificare la volontà negoziale.
A tal fine occorre ricordare che l'accordo quadro non deve essere strettamente vincolante (deve cioè essere limitato alla correttezza e buona fede) altrimenti si rientrerebbe nelle cosi dette "condizioni contrattuali generali"). Una fattispecie dell'accordo quadro è la joint venture.
Le parti dell'accordo rinviano poi la definizione alle singole intese delle parti con singoli piccoli accordi. Per tutto ciò che non viene espresso in queste intese viene preso come riferimento l'accordo quadro generale.

Silenzio: di solito non implica responsabilità, assume un duplice aspetto di:

1) Reticenza (non dire qualcosa che avrebbe potuto modificare o annullare il contratto) e assume rilevanza giuridica. Può incidere come vizio della volontà
2) Omessa Dichiarazione: assume rilevanza giuridica solo se richiamato contrattualmente o dagli usi o dalla legge diventando così "manifestazione di volontà espressa non tacita".

Lettera di Intenti: sono così chiamati tutti quei documenti con le quali le parti enunciano la loro intenzione di iniziare una trattativa. NON assumono carattere vincolante ma sono preliminari a una successiva a più completa fase di incontri. "Non costituisce alcun reciproco impegno od onere".

Verbali di Riunione: hanno la funzione di comprovare gli incontri avvenuti e di confermare l'attività svolta e quanto stabilito in sede di riunione. Se firmati hanno valore vincolante e possono modificare la natura del contratto. Hanno di per sé solo valore interno e possono eventualmente essere utilizzati con valore legale se sottoscritti dalle parti presenti. In mancanza di sottoscrizione (firma) hanno solo valore di riferimento per eventuali prove testimoniali. Infatti solo la sottoscrizione consente di riferire la dichiarazione a chi l'abbia effettuata.

Minuta o Bozza Contrattuale: è solo una proposta senza valore vincolante. È sempre opportuno però indicare che si tratta di "semplice bozza o minuta puramente indicativa e non vincolante". Infatti potrebbe intendersi la minuta o bozza come intesa sui soli elementi essenziali rinviandosi ad un momento successivo la determinazione degli elementi accessori e integrativi senza i quali l'esecuzione no sarebbe attuabile.

Offerte (di contratto): posso essere di tre tipi:
1) Offerta al pubblico: se ha tutti gli estremi essenziali del contratto cui è diretta ed è accettata vale come Proposta, resta salva la possibilità di revoca ("se comprate la macchina entro giugno la pagate…")
2) Promessa al pubblico: consiste nella promessa al pubblico di una prestazione in favore di chi si trovi in una determinata situazione o compia una determinata azione. Il vincolo giuridico sorge a fronte del semplice fatto di manifestare pubblicamente la propria volontà
3) Proposta contrattuale in senso diretto: è priva della esteriorizzazione "erga omnes" ossia verso tutti, propria delle altre due figure

Le offerte o proposte contrattuali assumono vero e proprio valore vincolante se hanno ALMENO una delle seguenti caratteristiche:
1) Irrevocabile
2) Contiene tutti gli elementi del contratto ed è accettata
3) Se modifica una precedente offerta/proposta diventando essa una nuova offerta/proposta ed è accettata

Cautele Legali nella richiesta di offerta:
1) Riservarsi il diritto di rifiutare in modo esplicito o implicito
2) Stabilire un termine entro il quale debba pervenire l'offerta
3) In eventuale gara riservarsi il diritto di accettare l'offerta più bassa
4) Prestabilire su chi graveranno le spese di predisposizione dell'offerta anche in caso di mancata stipulazione
5) Stabilire chiaramente che "il presente contratto costituisce manifestazione univoca e definitiva della volontà delle parti. Esso supera e annulla qualsiasi altro precedente accordo tra le parti".
6) Inserire tutto quanto avviene in fase precontrattuale come allegato al contratto.

Studio di fattibilità: è un contratto, un vero e proprio appalto, con un costo, che può essere fatto fare a terzi. Non è altro che un incarico professionale che verrà utilizzato, ad esempio, nello sviluppo di software. Nel caso di errori nello studio di fattibilità c'è una responsabilità anche per chi fa lo studio. Si incarica qualcuno di fare uno studio indipendentemente dall'oggetto dell'appalto. Le obbligazioni che si assume chi fa lo studio sono le stesse degli appaltatori. Ha una funzione di garanzia sul prodotto finale poiché l'appalto è un contratto a rischio di impresa. Rafforza le obbligazioni.

Penale: è una garanzia, una liquidazione anticipata del danno (deve essere correttamente misurata, non deve essere iniqua). Sono divise in due tipi:
1) Definitiva: si deve pagare ciò che viene stabilito
2) Temporale: in base al tempo si paga di più (al giorno). Si usano nello sviluppo del software
Le più utili sono le seconde. Non serve mettere delle penali assurde che mettono in ginocchio la controparte poiché si rischia di non prendere nulla

Tutela del software: il software è tutelato in maniera particolare. È un prodotto non un servizio, è un bene che serve per fare un servizio. Essendo un prodotto può essere difettoso e portare a conseguenze anche gravi.

Non è brevettabile, rientra nel copyright e nel diritto di autore. La legge sul diritto di autore tutela la forma e non l'idea.

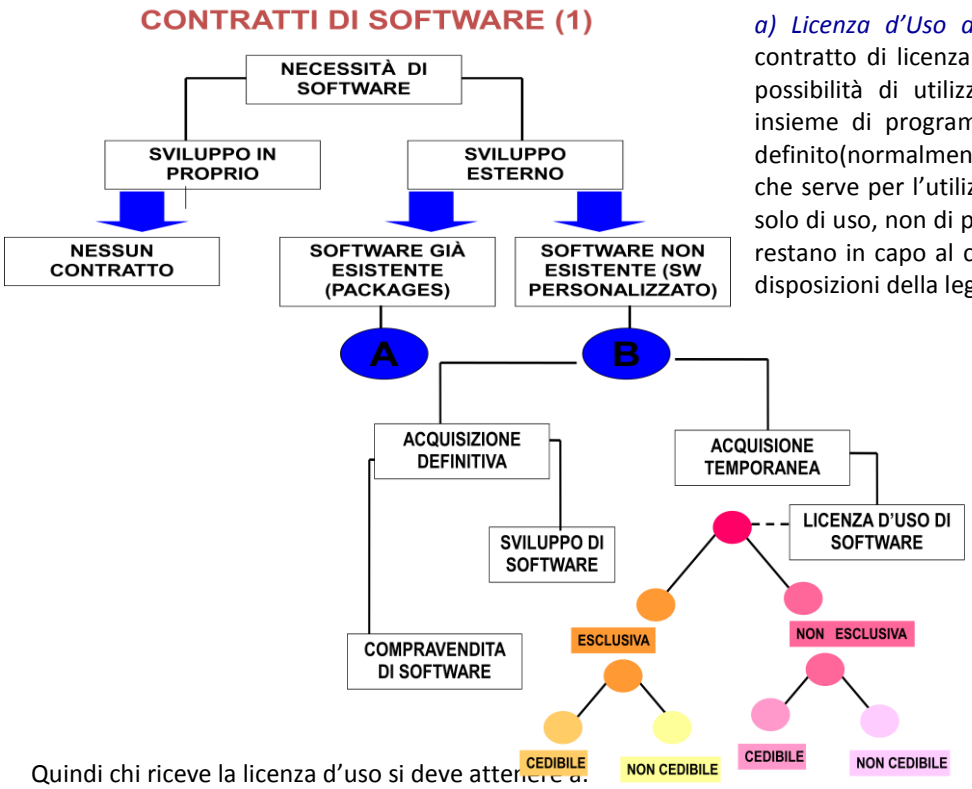
Lo sviluppo di software trasferisce tutto in capo al cliente. Se si modifica qualcosa serve la prova scritta.

Il software è tutelato da tre istituti giuridici, ossia tre "macrosfere" di tutela:

1. *Contrattuale*: che a sua volta si divide in
    a. *Disciplina Propria dei Contratti*: in caso di violazione prevede
        i. *Provvedimenti Cautelari*: sequestro
        ii. *Provvedimenti Definitivi*: sentenza di risoluzione contrattuale e condanna al risarcimento dei danni contrattuali e dei danni extra contrattuali.
    b. *Violazione del Principio di Concorrenza sleale*: commette concorrenza sleale chi si vale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda. In caso di violazione si incorre in:
        i. *Provvedimenti cautelari*: sequestro e ordinanza di sospensione commerciale
        ii. *Provvedimenti definitivi*: con sentenza di condanna che prevede la distruzione delle copie, il divieto di prosecuzione nell'attività economica commerciale, la condanna al risarcimento del danno e la pubblicità della sentenza
2. *Disciplina dei Brevetti*
3. *Copyright (Diritto d'Autore)*: il software viene equiparato in materia di legislazione sul diritto di autore a un opera letteraria ai sensi di quanto dispone l'art. 1 della Legge n. 633 del 1941. Questo pone dei problemi in quanto il software, tutelato perché considerato "opera letteraria", deve essere originale e quindi presentare un autonomo carattere creativo e risultare come un originale prodotto dell'ingegno del suo autore. Rispetto alle opere letterarie, la stessa natura funzionale e pratica del software impone una particolare valutazione del grado di originalità che lo stesso deve presentare ai fine della tutela. Il momento è di particolare rilievo dato che la scelta del criterio da adottare in sede di valutazione d'originalità, incide in modo rilevante sulla possibilità di ricorrere alla tutela giuridica. Il legislatore comunitario propende per un approccio di tipo soggettivo, disponendo che un programma per elaboratore è tutelato solo se originale, ossia se è il risultato della creazione intellettuale dell'autore. Il risultato di tale intervento legislativo è stato quello rendere meritevole di tutela ogni programma per elaboratore che risulti frutto di un'attività intellettiva dell'autore e non di una mera azione di copiatura. Restano esclusi dalla tutela accordata dalla legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma compresi quelli alla base delle sue interfacce. In altre parole: essendo il software essenzialmente un risolutore di problemi squisitamente tecnici e pratici, l'idea risolutrice non è di per sé tutelata dal diritto; quest'ultimo tutela, infatti, solo le diverse tipologie d'espressione attraverso cui si manifesta e si concretizza l'ingegno.

    In caso di violazione della Legge sul diritto di autore, i provvedimenti che possono venire presi sono di natura:
    a. *Civile*: viene preso un provvedimento di urgenza che sfocia in un accertamento e sequestro ed eventuale Sentenza definitiva penale
    b. *Penale*: con conseguente divieto di distribuzione del prodotto, divieto di ulteriore attività illecita, risarcimento del danno e pubblicità della sentenza.

Tipologie di contratti di software



a) Licenza d'Uso del software: L'elemento essenziale del contratto di licenza d'uso è il trasferimento all'utente della possibilità di utilizzare un pacchetto applicativo, cioè un insieme di programmi che costituiscono un prodotto ben definito(normalmente è oggetto di licenza tutto il materiale che serve per l'utilizzo del pacchetto applicativo). Il diritto è solo di uso, non di proprietà, quindi tutti i diritti di copyright restano in capo al concedente e l'utente deve attenersi alle disposizioni della legge sul diritto di autore.

Quindi chi riceve la licenza d'uso si deve attenere a:

- Legge sul diritto di autore (non può modificare il software)
- Accordi precisi con il concedente

PECULIARITA' della licenza d'uso: non trasferisce il diritto di proprietà, la titolarità e la possibilità di intervento sul software, solo di uso.

Licenza d'uso esclusiva è un mascheramento di commercializzazione (non incide sulla trasferibilità, potrebbe essere trasferito all'interno del gruppo o ad altre parti, ciò è determinato dalla cedibilità).

Le licenze d'uso a tempo indeterminato hanno tempo di pagamento a tempo indeterminato, se non c'è specificato nulla. Sono infatti caratterizzati dal pagamento UNA TANTUM, immediato.

È fatto divieto assoluto di:

1. (Peculiarità) Duplicare il programma (salvo copia di sicurezza)
2. Intervenire sul programma per modificarlo
3. Utilizzare il programma monoutente per pluriutente (sarebbe violazione della legge sul software ed eventualmente sulla cedibilità del contratto)

In materia di legislazione, si applicano per la licenza d'uso le norme relative alla locazione (affitto) degli immobili. La licenza d'uso è infatti un contratto non nominato atipico (ed è bene che sia scritto poiché la prova testimoniale di solito non vale come prova contro le condizioni scritte, si possono modificare le condizioni scritte solo con un altro contratto scritto). Inoltre, per la legge 110 sul diritto di autore, la trasferibilità dei diritti di natura economica DEVE essere scritta. Nei contratti misti bisogna sempre guardare quale figura contrattuale è prevalente per applicare le giuste leggi.

b) Contratto di Commercializzazione: fornisce la possibilità di distribuire il software in licenza a terzi. È caratterizzato da:

1. Accordo di distribuzione organico
2. Contratto "Tipo" di licenza (effettua delle duplicazioni autorizzate)

c) Sviluppo di Software: è un contratto nominato per codificato nel software. È un contratto di appalto, il software infatti è un bene non un servizio. Serve per effettuare un servizio. Lo sviluppo di software è nelle acquisizioni definitive poiché a fronte dello sviluppo del software tutto l'oggetto si traduce in capo al cliente, viene trasferita la titolarità del bene (lo dice l'appalto e non occorre la forma scritta per il trasferimento di titolarità); chi realizza il software non può tenere i sorgenti. Il pagare non incide sul contratto. L'effetto naturale del contratto di appalto è il trasferimento esclusivo (l'esclusività è data dal diritto di autore) di titolarità del prodotto realizzato. A volte, con una clausola di non concorrenza, la titolarità del software non viene trasferita ma è richiesta la forma scritta, è quindi possibile modificare il contratto con la forma scritta.

Esempio: pago una licenza 900k € e faccio fare lo sviluppo di un pacchetto relativo a questa licenza per 180k €, con trasferimento di titolarità. Quale figura contrattuale prevale? Nessuna sono due figure contrattuali distinte, legate da un continuum.

Inoltre se il software viene preso in licenza d'uso è un COSTO in bilancio, se è stato sviluppato è un PATRIMONIO poiché viene acquisito e l'ammortamento è differenziato con tassazioni differenti. Anche la posta a bilancio del bene può definire il genere del bene (licenza d'uso o patrimonio).

Chi sviluppa ha *due diritti (riconosciuti dal diritto di autore):*

1) Morale, ossia la paternità dell'opera (diritto forte riconosciuto come non distruttibile poiché la paternità non può essere trasferita, esiste solo la facoltà di disconoscere la paternità dell'opera)
2) Utilizzazione economica del bene

d) Manutenzione del Software: si distingue:

- *Ordinaria*: tende a eliminare i vizi insiti nel bene, correzione di errori, che non incide sulla struttura del software, è un service un appalto
- *Straordinaria*: indice sulla struttura stessa del software, si crea una figura contrattuale diversa che rientra nello sviluppo di software.

Infatti la manutenzione straordinaria tocca la struttura del software. È diverso da un semplice software ma è sviluppo di software, un appalto. Se il software è in licenza, allora è un appalto su un bene in licenza, non trasferisce la proprietà (come negli affitti).

Contratti di Services

Sono dei contratti di appalto, diversi dalla vendita (la vendita è relativa a un prodotto già esistente) sono degli appalti di realizzazione di prodotto o servizi su commissione. Hanno una peculiarità elevata.

a) Disaster recovery

Può esistere così com'è o inserito nell'Outsourcing. È un service dove qualcuno mette a disposizione di un cliente delle macchine nell'eventualità che il S.I. del cliente si blocchi. È un contratto aleatorio in due fasi:

1) Fase di durata generale: misurata in anni, in capacità elaborativa. È una forma di garanzia. Si paga un canone.
2) Periodo di disaster: nel caso di disastro si aiuta il cliente per il tempo di disastro con un costo.

Parte dei Test: si stabilisce che vengano fatte simulazioni. Chi effettua disaster recovery riceve dal cliente tutti i dati per testare il recupero dal disaster.

Natura Giuridica

Oggetto: Si tratta di una figura la cui natura giuridica è collocabile nell'ambito dell'appalto e specificatamente nell'appalto di servizi o misto (servizio + opera come nel caso in cui il fornitore sviluppi programmi appositamente per il cliente). DISASTER RECOVERY è l'accordo con una azienda specializzata nell'effettuare, usando strumenti e procedure adatte, il ripristino in tempi rapidissimi di tutte le attività informatiche soggette all'evento disastroso, in forza del quale sia possibile accedere immediatamente ad una porzione predefinita del sistema di emergenza, al fine di ripristinare le attività elaborative.

Natura contrattuale: Il Disaster Recovery ha per oggetto la prestazione di una attività di elaborazione su programmi dell'utente operanti sul sistema dell'offerente, e operante in situazioni di blocco, totale o parziale, del sistema informativo dell'utente medesimo. La figura è quindi caratterizzata dalla specifica funzione di "garanzia", cioè di "sicurezza" di continuità del ciclo vitale informativo anche a fronte di situazioni che ne hanno pregiudicato la regolare funzione per un periodo più o meno ampio.

Natura del contratto: caratteristica del D.R è quella di collocarsi indifferentemente come contratto singolo e autonomo da ogni ulteriore diversa prestazione oppure all'interno di un più complesso rapporto contrattuale, come ad es. Nell'ipotesi di outsourcing (e ciò sia come prestazione autonoma rispetto all'intera gestione del centro, sia come prestazione collegata / connessa alle altre)

Come opera: il Disaster recovery opera ponendo in essere un sistema di emergenza che investe le applicazioni vitali delle risorse elaborative dell'utente, risorse caratterizzate o dalla titolarità diretta in capo all'utente, o nella sola disponibilità dell'utente (o parziale titolarità di quest'ultimo, con riferimento cioè ai soli dati elaborati) nell'ipotesi di una maggior articolata situazione quale potrebbe essere la prestazione di un accordo di outsourcing

Modalità di prestazione: La prima opportuna regola da osservare è che l'Utente definisca correttamente le proprie esigenze tendendo conto dello stato attuale del suo sistema e delle possibili sue implementazioni e concordare detti parametri con il fornitore del disaster recovery. Il servizio di Disaster Recovery si concretizza in una serie di precise attività, tra cui primariamente, la presenza del sistema di emergenza e la sua disponibilità per il periodo di Disaster del sistema principale, la presenza di tutta la più o meno complessa, a seconda del tipo di accordo, attività di assistenza all'avviamento, la presenza di una serie completa di sistemi di sicurezza e quindi applicazione di tutti i sistemi di sicurezza e riservatezza e supporto per servizi ausiliari al personale dell'utente.

Garanzie:

A) il fornitore potrà garantire con polizza assicurativa i costi dell'utente per il servizio di recovery in caso di disastro
B) normalmente il fornitore garantisce solo la correzione di errori o vizi legati al programma e all'hardware, chiedendo di non rispondere per danni diretti dell'utente o di terzi

Durata temporale: l'arco temporale è distinto in tre diverse fasi:

A) Durata complessiva dell'accordo
B) Durata dell'attivazione dei test di prova
C) Durata del vero e proprio "servizio di emergenza

b) Facility Management

Oggetto del Contratto: Un articolato complesso di attività di service (prestazione di servizio) e di sviluppo (prestazione d'opera) rientra nell'ambito della figura contrattuale qualificata come Facility management. È un contratto quindi di prestazione di opera e di servizio con priorità alla prestazioni di accordi di Body Rental (utilizzo di personale della Società appaltatrice) e di consulenza sistemistica, ma ampliandosi sovente allo spazio operativo integrando la prestazione di servizio con la fornitura di software in licenza o di software e hardware in proprietà. L'accordo di FM può essere concluso:

- Direttamente fra il fornitore della prestazione di f.m. ed il cliente. Sotto questa ipotesi tutte le obbligazioni fanno capo ai due contraenti cioè al fornitore e al cliente che godranno dei corrispondenti diritti e obblighi
- Fra il fornitore di uno o più prestazioni ed un altro fornitore che, a sua volta, offrirà al cliente l'intero "pacchetto" di prestazioni. Sotto questa ipotesi il rapporto contrattuale può ulteriormente dividersi in:
    - Tutte le prestazioni vengono offerte da un solo fornitore che assume ogni obbligo e garanzia anche per le prestazioni fornite da altri fornitori, che, a sua volta garantisce per quanto riguarda le obbligazioni a carico del cliente
    - Tutte le prestazioni vengono offerte da un solo fornitore che assume ogni obbligo e garanzia anche per le prestazioni fornite da altri fornitori, che, a sua volta garantisce per quanto riguarda le obbligazioni a carico del cliente

In qualsiasi accordo di f.m. occorre prestare molta attenzione alle obbligazioni imposte da singoli fornitori nei loro contratti in modo da rendere omogeneo l'intero accordo e cioè vale sia per il rapporto fornitore cliente sia nel rapporto fornitore fornitore di FM.

Differenza dall'outsourcing: nell'outsourcing, che ne costituisce la più avanzata e completa forma, pur differenziandosi soprattutto per il fatto che nell'outsourcing solitamente non si perfeziona un'intesa di sviluppo di software, o, quantomeno ne costituisce una parte non preponderante, pur se a volte essenziale rispetto all'intera dinamica negoziale. riteniamo opportuno considerare l'Outsourcing come il limite estremo del Facility Management, intendendo però l'Outsourcing (come vedremo nelle pagine seguenti) come la scelta di spogliarsi completamente del proprio sistema informativo, e non come solo una o più deleghe tecniche al Fornitore, mantenendo la gestione diretta del proprio centro di calcolo e dati.

c) Outsourcing

c1) Natura giuridica

Natura del contratto: rientra nell'ambito del contratto d'appalto di servizio (o misto), pur se caratterizzato dalla più articolata presenza di una prestazione di opera vera e propria attuata con lo sviluppo di specifici programmi software atti a soddisfare le articolate esigenze dell'utente.

Oggetto del contratto: la fornitura di un completo servizio informativo che si sostituisca a quello dell'utente, praticamente in tutto o, quantomeno in materia preponderante, restando in quest'ultimo caso in capo all'utente medesimo solo attività marginali.

Se non c'è questa sostituzione completa o rilevante, quindi c'è una più ridotta distribuzione delle funzioni delegate non si parla di outsourcing ma la figura giuridica contrattuale cambia e la si colloca nell'ambito del Facility Management. Riteniamo che per considerare un accordo quale outsourcing sia necessario che una delle parti (il cliente/utente) si spogli del proprio sistema "integralmente" o comunque in modo rilevante,praticamente rinunciando alla gestione diretta del proprio centro e di quanto ad esso connesso(infatti qualsiasi classificazione terminologica è suscettibile di veridicità, e assume reale incidenza la sostanziale natura del rapporto posto in essere e non la sua qualificazione terminologica).

Peculiarità: è una figura contrattuale caratterizzata dalla presenza di un alto "rischio", cioè del pericolo che il trasferimento del sistema informativo vincoli l'utente in maniera estremamente rigida, condizionandone la futura eventuale scelta di ritorno alla gestione diretta. Dato l'alto rischio è bene quindi che prima di stipulare un contratto di outsourcing venga fatto uno studio di preliminare di fattibilità e/o un audit che può essere fatto dall'utente, dal fornitore o congiunto dal quale scaturiscano responsabilità in ordine all'esecuzione successiva dell'accordo assumendo incidenza ai fini dell'accordo definitivo e anche garanzie, che si riverberano dalla fase preliminare alla esecuzione finale dell'accordo di Outsourcing.

Le garanzie sono strettamente collegate all'oggetto sia per l'incidenza che per la decorrenza. Possono essere :

- Di servizio (errori, continuità)
- Correttive

Inoltre dal momento che il contratto di Outsourcing rientra nella ampia categoria dei contratti di appalto, occorre valutare anche l'incidenza della complessità contrattuale che fa capo alle esigenze dell'utente e che corrisponde alla fitta rete di interconnessioni negoziali in essere: così dovranno essere presi in considerazione altri rapporti contrattuali (vedi sotto). L'outsourcing è caratterizzato dalla Potenzialità del suo oggetto che ne condiziona i riflessi giuridici.

Oggetto del contratto: è un contratto di servizio che prevedere l'acquisizione (temporanea o definitiva) di beni. Essendo un servizio ed essendo quindi diretto a soddisfare precisi interessi, ha un oggetto di carattere "espansivo", occorre quindi di volta in volta determinare tecnicamente e giuridicamente la portata del contratto.

Rapporti contrattuali: il contratto di outsourcing è un contratto di servizio complesso. È un contratto di appalto (quindi implica sempre il parere favorevole del committente qualora si debba ricorrere al subappalto) di servizio che vede però la presenza potenziale di numerose altre forme contrattuali sulla quale predomina quella di outsourcing. Le altre forme contrattuali che possono essere presenti sono:

- con il gestore del servizio di Outsourcing stesso
- di (eventuale) sviluppo software
- di (eventuale) assistenza/manutenzione software
- di (eventuale) assistenza/manutenzione hardware
- di Disaster Recovery
- di ulteriori servizi di telecomunicazione
- di trattamento e/o trasmissione dati personali
- Ulteriori Servizi che si rendessero utili o che venissero richiesti dalla natura dell'accordo o dalla volontà del cliente.

Riduzione dell'area di rischio: come già detto, l'outsourcing è un contratto rischioso che è per sua natura, caratterizzato da una profonda incidenza pratica e non solo giuridica, nella sfera dell'utente e che quindi presenta una notevole "area di rischio". Per ridurre questa area di rischio:

- Occorre che sia sempre presente la possibilità di ripristino della situazione originaria o il passaggio dal fornitore originario ad un altro fornitore, il tutto senza particolari intoppi, e senza "rischio": rischio che grava indubbiamente sull'utente, ma che potrebbe riversarsi anche sul fornitore qualora, per sua scelta o per fatto indipendente ma comunque gravante su di lui, si rendesse necessario risolvere anticipatamente il contratto senza arrecare alcun danno all'utente. Quindi occorre che diventi condizione abituale determinare nel testo contrattuale le modalità di ripristino del sistema originario dell'utente o di sostituzione del fornitore in modo tale che, pur a fronte di ulteriori costi, l'utente abbia la certezza di non perdere mai il servizio di outsourcing
- Occorre valutare i contratti in vigore, particolarmente i contratti di titolarità software o di licenza d'uso, o comunque di durata come l'assistenza Software o manutenzione hardware. In relazione al contratto di outsourcing
- Occorre valutare la compatibilità fra il contratto di outsourcing con l'utente ed altri accordi del fornitore già in essere

Per far ciò è bene modificare nel contratto le Condizioni Generali e le Condizioni Speciali in maniera opportuna.

Clausole Generali e Speciali del Contratto:

Ciascun utente e ciascun fornitore presentano caratteristiche e necessità proprie. Ciascuna delle parti quindi trasmigrerà nell'accordo le proprie peculiarità, in considerazione delle personali caratteristiche ed esigenze, in modo tale da aver sempre presente l'obbiettivo da perseguire e di coordinare l'intera attività in modo uniforme e coerente, senza intoppi iniziali, durante la fase operativa del service e tanto meno nella eventuale fase di cessazione o rinegoziazione dell'intesa stessa. Richiamiamo alcune delle più comuni clausole di portata Generale o Speciale:

A) Condizioni Generali

A.1 - Prodotti e materiali del Fornitore e modalità dell'eventuale utilizzo dei prodotti e/o materiali del fornitore
- Proprietà
- Diritti Di Autore
- Brevetti

A.2 Prodotti e materiali dell'Utente

A3 - Ambiente operativo del Fornitore

A4 - Accesso fisico al centro: garanzie richieste all'utente per proprio personale

A5 - Sicurezza e riservatezza: informazioni e dati reciproci

A6 - Violazione di brevetti e copyright: il fornitore deve garantire la continuità del servizio anche a fronte di un eventuale contenzioso di tale natura. In particolare si richiede sempre l'assenso scritto per utilizzo di marchi o brevetti.

A7 -Divieto di subappalto: non sono ammesse attività di subappalto salvo espressa deroga

A8 - Corrispettivi e fatturazioni:
- Modalità
- interessi moratori
- tolleranza

A9 - Responsabili del progetto
- Indicazione
- sostituibilità
- poteri

A10 – Penali

Accessorietà rispetto ai rimedi ordinari a fronte di inadempimento

A11 - Clausola risolutiva espressa
- A reciproco favore a carico
- estremi di applicabilità

A12 - Foro competente
- Foro
- clausola
- alternatività per alcuni punti

A13 - Divieto di cessione
- Totale (per l'accordo e diritti)
- parziale (esclusione dei crediti da corrispettivo)

A14 - Modifiche e contenuto contrattuale
- Superamento di ogni precedente intesa
- modifiche solo scritte (e approvate)

A15 - Assicurazioni:
- Beni
- personale

B) Condizioni Speciali

La natura stessa dell'outsourcing implica la formulazione di condizioni contrattuali del tutto particolari, legate alla peculiarità delle prestazioni volute dalle parti. L'attenzione, come già scritto dovrà estendersi all'oggetto dell'accordo, che costituisce il fulcro dell'intesa e soprattutto alle modalità tecniche del servizio. Queste ultime dovranno ricomprendere anche alcuni punti essenziali per una positiva esecuzione dell'accordo, e precisamente:
- tipologia
- tempificazione
- soluzioni alternative
- richiesta di uniformità a standard
- test
- collaudo: critico poiché è importante stabilire come deve avvenire il collaudo, modalità e termini, approvazione.
- sistemi di sicurezza

Le condizioni particolari modificano il tipo di contratto. Nel contratto possiamo quindi indicare tempi di risposta del servizio, si indicano praticamente le modalità tecniche del servizio. Oggetto: è il cuore dell'accordo, indica cosa bisogna fare e come deve essere fatto, (Allegato tecnico deve essere esaustivo, se c'è lo studio preliminare si richiama o si inserisce nell'oggetto stesso). Il collaudo è.
Problemi da risolvere nel servizio devono essere: continuità del servizio (se ci sono tempi morti vanno stabiliti), errori (che si solito nascono nel caso di applicazioni specifiche per sistemi collaudati).
Audit (controllo) sul fornitore da fare prima e durante il contratto per verificare le prestazioni. Tendenzialmente è pagato dal cliente, verifica come vengono effettuate le cose dal fornitore.

L'outsourcing è una attività a rischio, quindi va controllata attentamente dagli amministratori.

Note aggiuntive

Facility management e Outsourcing sono service, sono solitamente dei contratti misti (Prestazione di Servizio + Sviluppo Software e/o licenza d'uso + Disaster Recovery verso una terza parte). Rimane preponderante la figura dell'appalto di service. Evita al cliente continui aggiornamenti HW e SW,ha dei vantaggi di costo economici ma è rischioso. Ci deve essere la possibilità di fare ritorno a usare i propri sistemi, il cliente deve essere in grado di poter salvare i dati magari tramite disaster recovery (nel capitolato tecnico è bene mettere tutto ciò che è in grado di tutelare me stesso e il mio datore di lavoro).

L'appalto è caratterizzato dall'Inducto Ad Personam, cioè da un rapporto con un specifica persona. In caso di cambio di questa persona può essere richiesta la rescissione del contratto.

Due cose importanti in questo tipo di contratto:
1) Valutazione della possibilità di trasferire e terminare il rapporto
2) Valutazione della possibilità di ripristinare il sistema

Criminalità Informatica LEGGE 22.12.1993 N.547

Prima dell'attuale legge si riteneva che i reati informatici potessero distinguersi in due categorie generali:

a) *crimini perpetrati con l'ausilio di apparecchiature informatiche*
b) *crimini perpetrati contro apparecchiature e programmi informatici*

Si riteneva inoltre che per i reati informatici potesse valere sicuramente il richiamo ai "crimini economici", ma che una collocazione forzosa in detta categoria potesse rivelarsi incompleta o, per molteplici situazioni non calzante, in quanto ritenevamo che tale elemento economico non fosse una"costante" della fattispecie.

Classificazione dei reati informatici

Si possono classificare in:

1) *Danneggiamento*: intendendosi con tale termine le azioni criminose attuate:
   a) *contro : hardware, contro software, contro il complesso dei mezzi di comunicazione*
   b) tramite l'alterazione di dati in modo da produrre un danno all'utilizzatore o a terzi
   Le due categorie possono, a loro volta, compenetrarsi vicendevolmente e non escludersi, aggravando così la situazione del soggetto leso
2) *Alterazioni di informazioni* atte ad impedire l'esatto uso di nastri, dischi o programmi e particolarmente: il Superzapping, il Data Dilling, il Trojan horse, l' Asyncronous attack, la Logic Bomb
3) *Virus*: sono caratterizzati da un comportamento tale da dar luogo a molteplici situazioni, quali, ad esempio, la cancellazione di precisi programmi, la creazione di "bad sectors", l'assorbimento di memoria, la formattazione, l'impedimento di operatività del sistema. Sono distinti in:
   a. *Virus maligni o letali*: caratterizzati da un elevato livello di pericolosità in quanto inducenti danni irreversibili o comunque difficilmente o difficoltosamente rimediabili
   b. *Virus benigni o non letali*: caratterizzati invece da un elevato livello di fastidio .

Nel Penale non esiste il principio di ricorso per analogia (c'è il divieto di applicazione del principio, difatti le nuove norme introdotte non hanno efficacia retroattiva, non si può essere puniti per azioni compiute prima dell'ingresso della legge e che prima non erano reato), in civile si-> fattispecie del codice penale non prevedevano reati informatici.
Legge n. 547 crea una norma per punire i reati informatici (precedentemente in assenza di una norma penale precisa non si potevano applicare sanzioni).
Prima c'era solo l'art 420 ch puniva attentato a impianti di pubblica utilità, erano escluse se altre fattispecie di impianti.

Art 491: Documenti informatici

Venne introdotto l'art 491 per introdurre i documenti informatici poiché non erano "conosciuti" dalla legge. L'articolo definisce cosa è un documento informatico e divide in due classi i documenti informatici:

1) *In senso stretto*: supporto informatico contenente dati o informazioni aventi efficacia probatoria, destinato a essere letti dall'elaboratore
2) *Non in senso stretto*: programmi destinati a elaborare documenti informatici in senso stretto

Ed inoltre dice che " Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private", ossia applica le norme dei diritto degli atti pubblici e delle scritture private ai documenti informatici.

Elemento Soggettivo: il dolo di violare il principio della pubblica fede e il dolo di violare la scrittura privata.

Distinguiamo in colpa e in dolo in base all'intenzionalità di commettere reato:
Dolo: intenzione che ha il soggetto di commettere reato, con la coscienza di commetterlo. Si divide in:
Generale: tengo una determinata condotta, non c'è volontarietà specifica
Specifico: Specifica condotta e motivo, dice proprio per quale motivo tengo una precisa condotta, c'è la volontarietà specifica
Colpa: non ho la coscienza, non c'è intenzionalità

Frode informatica: è richiesta l'alterazione o la distruzione per passare al reato di frode informatica e l'ingiusto profitto (patrimoniale o no) a danno di qualcun altro.

Reato qualificato: può essere commesso solo da una certa categoria.

Fuori dai casi consentiti dalla legge -> per difesa della legge, di fronte all'interesse comune.

Art 615ter: accesso abusivo a un sistema informatico

è considerato come violazione di domicilio ma di fattispecie informatico. *Le aggravanti prevedono la qualifica della persona che lo commette*. Le misure di sicurezza non devono essere elevate, *basta la non volontà del soggetto che subisce intrusione*. Non è necessario un fine preciso, non serve che l'intrusione sia finalizzata a qualcosa. Inoltre il danno non deve essere fatto effettivamente, basta la potenzialità del reato. L'elemento oggettivo è costituito dal comportamento di accesso "indiscreto", ma a condizione che il sistema goda di misure di sicurezza. deve sussistere la volontà di escludere l'introduzione da parte dell'autore del reato in detti "luoghi". La volontà di esclusione può risultare in modo espresso o comunque inequivocabilmente manifesto: come nell'ipotesi di divieto di accesso agli strumenti informatici o telematici , divieto che può benissimo desumersi anche dal compimento di atti incompatibili con il comportamento di chi si introduca. In pratica basta che si sia la volontà del titolare del diritto al rispetto delle norme.

Consenso putativo: devo credere (essere certo) che avevo il diritto di entrare e il consenso altrui a farlo.

Bisogna quindi fare attenzione e distinguere due casi:

1) *Dissenso tacito*: postula una manifestazione ostativa di volontà, percepita come tale dall'agente
2) Dissenso presunto: prescinde da una manifestazione ostativa di volontà, che non è percepita come tale dall'agente

Infatti nel secondo caso, il dissenso presunto non può ritenersi sufficiente per l'esistenza del reato

615quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Anche la diffusione di chiavi di accesso procurate abusivamente e le diffonde contro il volere del proprietario per procurare a se o ad altri profitto (anche non monetario) viene condannato (ci devono essere tutte le componenti: condotta – fine).

Danneggiare si intende anche allo stato potenziale, integra comunque la condotta del reato.

615quinquies. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

616. Violazione, sottrazione e soppressione di corrispondenza (Diritto alla segretezza e all'inviolabilità della corrispondenza)

Punibile a querela della persona offesa = Se il soggetto che ha subito danno non ci denuncia non siamo perseguibili.

Segreto: qualsiasi informazione o notizia che gode di tutela nei confronti di chi voglia rendere pubblica la notizia al di fuori dell'effettivo titolare.

La presa cognizione del contenuto non implica la lettura del documento.

Delitti vuol dire che sono punibili con l'ergastolo.

617quater. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.

L'elemento caratterizzante è offerto dal comportamento "fraudolento" cioè in violazione del principio di correttezza e di lealtà, e quindi, in assenza non solo di consenso, ma attraverso l'utilizzo di sistemi o mezzi che ingannano i titolari dei diritti (informazioni) alterando il regolare sistema di trasmissioni.

Il dolo consiste nel semplice fatto di intercettare, impedire o interrompere il flusso di informazioni

617quinquies. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Il dolo è specifico ed offerto dalla volontà di installare allo scopo di perseguire l'intercettazione, l'impedimento o la interruzione

617sexies. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.

L'elemento oggettivo è offerto dalla formazione, modificazione o soppressione totale o parziale del contenuto della comunicazione ,in qualunque modo avvenga purché caratterizzato dal dolo specifico di ottenere il vantaggio o di arrecare danno, e il tutto legato all'uso del contenuto della comunicazione, qualunque sia stato il modo della ricezione

621. Rivelazione del contenuto di documenti segreti

Viene estesa la tutela propria del documento segreto anche a "qualunque supporto informatico contenente dati, informazioni o programmi. L'interesse tutelato è ovviamente quello "al segreto" cioè al diritto di escludere i terzi dalla conoscenza di fatti o notizie, però con l'indicazione che l'interesse al segreto è nei confronti di qualcosa di nuovo rispetto al precedente concetto di documento, e cioè "il supporto informatico" .

Il reato è qualificato dal dolo specifico, almeno per quanto concerne l'impiego del contenuto del documento, e quindi, si richiede la consapevolezza e la volontà di rivelare il detto contenuto.

623bis. Altre comunicazioni e conversazioni

Estende la tutela del diritto alla libertà e inviolabilità del segreto, a tutti i casi e non più solo a quanto effettuato con "collegamento su filo o onde guidate".

Art.635 bis- Danneggiamento di sistemi informatici e telematici

Il dolo richiesto è generico, occorrendo semplicemente la volontà di danneggiare indipendentemente dal fine che si sia proposto l'autore dell'atto criminale, e quindi non è richiesto il dolo specifico. . Il danno deve essere tale da integrare una pur minima modifica strutturale o funzionale del bene o implicarne un pur minimo deterioramento.

640. Truffa

L'interesse tutelato dall'articolo in esame si identifica, da un lato, nel bene inteso come patrimonio-prodotto, e dall'altro, nella buona fede. L'elemento oggettivo è offerto dall'estensione del concetto di frode, così come contemplata dagli artt.513 -517 c.p., sottolineandosi altresì come lo stesso titolo dell'articolo indica. L'elemento soggettivo è offerto dalla concezione tradizionale per la truffa con il dolo generico, e quindi con l'interconnessione di tutti gli elementi oggetto del dolo (tra cui: inganno, disposizione patrimoniale, ingiusto profitto)

Forme di Criminalità in Internet

a) attività criminali dirette contro i sistemi telematici
b) attività criminali poste in essere attraverso i sistemi telematici
c) attività criminali dirette contro i sistemi telematici e con sistemi telematici.

La loro collocazione in una categoria specifica di reati dipenderà poi dalla loro natura, ed in linea di massima possiamo classificarli come segue:

a) Reati contro la proprietà intellettuale in senso lato: Detti reati comprendono tutte le fattispecie di duplicazioni abusive (illecite) di beni tutelati dal Diritto d'Autore : violazioni del software, delle video produzioni, delle produzioni sonore, dei diritti librari ed editoriali ecc…
b) Reati contro precise norme di tutela dei dati (violazione della privacy) o delle banche dei dati (entrambi su base legislativa specifica, come ad esempio la L. 31.12.1996 n. 676)
c) Reati contro le norme di sicurezza imposte in settore rilevanti, quali nell'ambito delle telecomunicazioni.
d) Reati compiuti tramite internet ma di natura per così dire generale : come, ad esempio, la truffa , la truffa in commercio, il furto tramite utilizzo di carte di credito acquisite illegalmente tramite internet.
e) Reati così detti di diffamazione o di estrinsecazione del pensiero: si tratta, in quest'ultimo caso, di figure particolari, che prima dell'impatto di internet, si collocavano in un ambito per così dire più ristretto : quello delle comunicazioni dirette interpersonali, o tramite l'uso della carta stampata o dei canali televisivi in genere.

600 ter c.p. (Pornografia minorile), 600 quater c.p. (*Detenzione di materiale pedopornografico)* , 600 quinquies c.p. *(Iniziative turistiche volte allo sfruttamento della prostituzione minorile)*

Soggetti interessati alle operazioni su internet

- il **fabbricante**: è sicuramente l'anello forte della catena, giacchè , salvo ipotesi di case farmaceutiche " pirata", solitamente chi opera nel settore è ben attento alle norme e leggi in materia, sia nazionali che sovranazionali.
- il **gestore del sito**: non necessariamente si identifica con il fabbricante, e quindi è il soggetto che potrebbe incorrere nella sanzione distribuendo (e vedremo poi in che senso) il prodotto.
- il **provider**: come noto (e sempre oggetto di vivace discussione) la posizione del provider risente del suo rapporto diretto con l'informazione che trasmette. Salvo che non abbia conoscenza del fatto che, tramite suo, vengano trasmesse informazioni costituenti reato (come ad esempio nell'ipotesi di pornografia infantile trasmessa via Internet), nella fattispecie non dovrebbe risentire di sanzioni, in quanto l'introduzione in Italia del prodotto privo dell'autorizzazione avviene , solitamente, tramite **uno spedizioniere** che, a sua volta, per evitare incriminazioni, dovrà rispettare le norme vigenti in tema di dichiarazioni doganali.

Bisogna sempre valutare il mezzo internet cioè se esso operi:

a) come "strumento diretto" per l'attuazione del fatto criminoso,
b) opera alla stregua di un comune mezzo di comunicazione

Locus Commissi Delicti: per i crimini commesse sfruttando internet, vale il principio di Territorialità del Crimine, ossia si applicano le leggi dello Stato in cui è iniziato il crimine. Fanno eccezione a questo principio alcuni reati come il Riciclaggio di Denaro e la pedopornografia.

Codice della Privacy (D.Lgs. 196/2003) sul trattamento dei dati personali

Oggetto della Legge è il trattamento del dato.

Diritto alla riservatezza (autodeterminazione informativa) è sinonimo di diritto di controllare le informazioni personali.

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (elemento identificativo dell'interessato).

> *Dati identificativi*: i dati personali che permettono l'identificazione diretta dell'interessato;
> *Dati sensibili*:, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
> *Dati giudiziari*: i dati personali idonei a rivelare provvedimenti ..o la qualità di imputato o di indagato ai sensi …

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Chi tratta il dato è quel soggetto che decide come deve essere trattato il dato. Il responsabile del trattamento è delegato dal titolare, ha meno responsabilità. La sua responsabilità è trattare i dati in maniera confermo a quella dettata dal titolare e in maniera corretta. Il titolare del trattamento è chi conferisce all'impresa di Service il dovere di trattare i dati. Titolare e Responsabile possono essere due figure in un certo senso intercambiabili.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.
Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

I dati sensibili sono delicati, per il trattamento di questi dati è necessario:

1) Il consenso scritto dell'interessato
2) La garanzia di sicurezza nel trattamento dei dati da parte di chi tratta i dati.

L'interessato può in qualunque momento intervenire e modificare/revocare il consenso.

Sicurezza dei Dati e dei Sistemi

Le misure adottate dovranno proteggere I DATI PERSONALI ED I SISTEMI e cioè:

- Programmi informatici
- Gli strumenti elettonici e non
- Il sistema informativo nel suo complesso
- Atti e docuenti cartacei
- Gli archivi (informatici e non)

Obblighi di sicurezza riguardano:

- Il titolare del trattamento
- Il responsabile (se è stato nominato)
- Gli incaricati
- E qualunque altro soggetto che e' tenuto all'adozione delle misure di sicurezza

Il titolare dovra':

- Vigilare e verificare che le informazioni da lui impartite siano rispettate
- Nell'applicazione delle misure di sicurezza dovrà tenere conto dell'articolo 15 del codice per effetto del quale nel caso di richiesta di risarcimento danni dovrà dimostrare di aver adottato tutte le misure idonee ad evitare il danno

La protezione dei dati personali attraverso adeguate misure di sicurezza è prevista in più parti del codice. Sono state previste nuove misure di sicurezza. Rimane la differenza (ugualmente al testo previgente) tra i trattamenti svolti con strumenti elettronici (art. 34) e quelli effettuati senza l'ausilio di tali strumenti (art. 35).

Art. 15: in caso di danno arrecato ad altri per effetto del trattamento dei dati personali il risarcimento viene effettuato ai sensi dell'articolo 2050 ossia si equipara l'attività di trattamento dei dati personali a un attività pericolosa, se non dimostra di aver adottato tutte le misure idonee ad evitare tale danno. La peculiarità di tale articolo è inoltre il cambiamento del criterio di imputabilità che si traduce *nell'inversione dell'onere della prova* a carico di colui che svolge l'attività pericolosa, invece che al danneggiato (il danneggiato deve solo dimostrare di aver subito un danno, Il danneggiante dovrà dimostrare di aver predisposto ogni accorgimento necessario tale da escludere il nesso eziologico, ossia il nesso di causalità tra le cause e l'evento, tra l'attività pericolosa di trattamento dei dati e l'evento.

Il titolare ed il responsabile dovranno perciò adottare le misure di prevenzione più idonee, oltre a quelle minime prescritte, tra quelle disponibili in relazione alle conoscenze acquisite ed allo sviluppo delle tecnologie, allo scopo di ridurre al minimo i rischi, possibili, probabili, prevedibili e prevenibili che incombono sui dati.

L'inosservanza delle norme sulla sicurezza potrà comportare responsabilità civili e penali da parte del titolare, del responsabile o di chiunque, essendovi tenuto, ometta di adottarle:

a. penali: se non sono adottate le misure minime;
b. civili: con risarcimento del danno in assenza di quelle più ampie che dovranno risultare sempre aggiornate.

Risarcibilità del danno non patrimoniale: il danno morale (non patrimoniale) sarà risarcibile SOLTANTO COME PREGIUDIZIO EFFETTIVAMENTE CONSEGUENTE AD UNA LESIONE.

i soggetti tenuti a rispondere dei danni cagionato per effetto del trattamento sono titolare ed al responsabile del trattamento in funzione alla loro capacità di decidere in merito alle fasi del trattamento o alle operazioni che hanno causato o permesso la realizzazione del danno. In particolare per ciò che concerne il titolare del trattamento si ritiene che possa essere considerato responsabile tanto la persona fisica quanto quella giuridica, quanto la PA

Nuovi Delitti in relazione alla tutela della Privacy:

- 167 *(Trattamento illecito di dati);*
- 168 *(Falsità nelle dichiarazioni e notificazioni al Garante);*
- 170 *(Inosservanza di provvedimenti del Garante).*

Tutti i delitti contengono una "clausola di salvezza" – *"salvo che il fatto costituisca più grave reato"*; Pena edittale minima; Non è permesso l'utilizzo delle misure cautelari e di strumenti di investigazione come ad esempio le intercettazioni telefoniche.

Appunti Aggiuntivi sul Software

Il software è un bene e rientra nell'ambito di quei beni che possono essere Difettosi. Scatta quindi la Responsabilità Oggettiva.

La tutela del software è di due tipi:

- Contrattuale
- Diritto di autore (molto forte) che si divide in:
  - Diritto Morale, fortissimo, non cedibile (come la paternità che non è cedibile ma solo disconoscibile)
  - Diritto Patrimoniale

Si applicano le norme penali anche al Software (ossia si applica il diritto di autore in sede penale)

Riepilogo Articoli

Art.	Soggetto	Cosa deve fare	Con che fine	Punito con:	Aggravanti	Ulteriori Aggravanti / Note
615ter. Accesso abusivo ad un sistema informatico o telematico	Chiunque	abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo	(nessuno in particolare)	Reclusione fino a tre anni	1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente 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, delle informazioni o dei programmi in esso contenuti.	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 o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
615quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.	Chiunque	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	al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente	reclusione sino a un anno e con la multa sino a euro 5.164	La pena è della reclusione da uno a due anni e 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'articolo 617quater	
615quinquies. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.	Chiunque	diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento	danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento	reclusione sino a due anni e con la multa sino a euro 10.329		
616. Violazione, sottrazione e soppressione di corrispondenza	Chiunque	prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime	al fine di prenderne o di farne da altri prender cognizione	se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516	Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni . Il delitto è punibile a querela della persona offesa	Agli effetti delle disposizioni di questa sezione, per «corrispondenza» s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza
617quater. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	Chiunque interviene e chiunque diffonde	fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe		reclusione da sei mesi a quattro anni	Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa . Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.	

617sexies. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche	Chiunque	forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi	al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno	è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.	La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617quater	
621. Rivelazione del contenuto di documenti segreti	Chiunque	essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza [6164], lo rivela, senza giusta causa, ovvero l'impiega	a proprio o altrui profitto	è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni (1) o con la multa da euro 103 a euro 1.032	Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi . Il delitto è punibile a querela della persona offesa	
623bis. Altre comunicazioni e conversazioni.		Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati				
Art.635 bis- Danneggiamento di sistemi informatici e telematic	Chiunque	distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi o informazioni o dati altrui		è punito, salvo che il fatto costituisca più grave reato , con la reclusione da sei mesi a tre anni	Se ricorre una o più delle circostanze di cui al comma 2 dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni	
640. Truffa.	Chiunque	con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno		è punito con la reclusione da sei mesi 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 : 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare [c.p.m.p. 162, 32quater] 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità . Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante	
600 ter c.p. (*Pornografia minorile) Comma 1*	***Chiunque***	***sfrutta minori degli anni diciotto alò fine di realizzare esibizioni pornografiche o di produrre materiale pornografico***		***reclusione da sei a dodici anni e con la multa da €. 25.822 a € 258.228 .Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma***		
Comma 2	***Chiunque***	***con qualsiasi mezzo anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o alo sfruttamento sessuale di minori degli anni diciotto***		***reclusione da uno a cinque anni e con la multa da € 2.582 a €.51.645.***		

Comma 3	***Chiunque***	***al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni 18***		***reclusione fino a tre anni o con la multa da € 1.549 a € 5.164***		
600 quater c.p. (*Detenzione di materiale pedopornografico)*	***Chiunque***	***consapevolmente , procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale di minori degli anni diciotto***		***reclusione fino a tre anni o con la multa non inferiore a € 1.549***		
600 quinquies c.p. *(Iniziative turistiche volte allo sfruttamento della prostituzione minorile)*	***Chiunque***	***organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione in danno di minori o comunque comprendenti tale attività***		***reclusione da sei a dodici anni e con la multa da € 15.493 a € 154.937***	*Le disposizioni di questa sezione , nonché quelle previste dali articoli 609 bis (Violenza sessuale), 609 ter(Circostanze aggravanti), 609 quater (Atti sessuali con minorenne) e 609 quinquies (Corruzione di minorenne) , si applicano altresì quando il fatto è commesso all'estero da cittadino italiano, ovvero in danno di cittadino italiano, ovvero da cittadino straniero in concorso con cittadino italiano. In quest'ultima ipotesi il cittadino straniero è punibile quando si tratta di delitto per il quale è prevista la pena della reclusione non inferiore nel massimo a cinque anni e quando vi è stata richiesta del Ministero di grazia e giustizia*	