LEGGE 22.12.1993 N.547
CONTRO LA
CRIMINALITA' INFORMATICA

"REATI INFORMATICI"

Corso di diritto dell'informatica

REATI INFORMATICI

- Precedentemente alla normativa in oggetto si riteneva che l'attenzione degli interpreti dovesse accentrarsi su un'area ristretta , interessata dal rapporto “strumento informatico- crimine" e quindi 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 nessuno dubitava che vi fosse in simili reati un elemento “patrimoniale" quale spinta all'esecuzione del fatto criminoso, ma ritenevamo altresì che tale elemento economico non fosse , in ultima analisi, una”costante" della fattispecie.

REATI INFORMATICI

- In assenza di un dettato normativo nazionale, apparso come visto solo nel 1993, ritenevamo che tutte le classificazioni, pur imperfette, dei reati informatici, dovessero necessariamente tener conto di quanto sviluppato dagli esperti della sicurezza tecnica e dell'audit informatico negli USA ed in altre Nazioni all'avanguardia nel settore , e su tale base parlammo di:
- 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 potevano, a loro volta, compenetrarsi vicendevolmente e non escludersi, aggravando così la situazione del soggetto leso.
- Le modalità concrete di attuazione del danneggiamento potevano essere le più svariate , tra cui le rotture volontarie, le esplosioni, il calore, il freddo e così via.

REATI INFORMATICI

- 2. Vi erano poi le *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' Anasyncronus attack
- la Logic Bomb
- 3) Virus
- Una menzione a parte veniva dedicata ai così detti *virus informatici,* che oggi argomento notissimo, alla fine degli anni ottanta apparivano prepotentemente all'attenzione degli utenti e degli operatori informatici.
- Il termine “Virus" venne mutuato dal linguaggio medico per la particolare assonanza del fatto informatico con la capacità di propagazione delle malattie virali ed il paragone si mostrava quanto mai calzante stante la capacità di diffondersi di ciascun virus informatico e la sua spiccata tendenza a invadere sempre nuovi spazi.
- D'altronde il Virus Informatico altro non è che un vero e proprio programma in grado di intaccare altri programmi così come nella realtà medica i virus infettano via via più soggetti man mano che questi ne vengano in contatto.

REATI INFORMATICI

- Distinguevamo inoltre i Virus Informatici in due primi grandi gruppi:
- *a) Virus maligni o letali*
- *b) Virus benigni o non letali*
- essendo i primi caratterizzati da un elevato livello di pericolosità in quanto inducenti danni irreversibili o comunque difficilmente o difficoltosamente rimediabili, ed i secondi caratterizzati invece da un elevato livello di fastidio .
- Pertanto i Virus Informatici sono caratterizzati da u comportamento tale da dar luogo a molteplici situazioni, quali, ad esempio, la cancellazione di precisi programmi, la creazione di "bad rectors", l'assorbimento di memoria, la formattazione, l'impedimento di operatività del sistema.

REATI INFORMATICI

- Visto il divieto di applicazione in materia penale del principio di “analogia” si poneva agli interpreti un ostacolo difficilmente sormontabile e cioè l'assenza di una specifica disposizione di legge che inquadrasse le fattispecie di reati qualificati come informatici, non potendosi, diversamente, in forza del divieto di applicazione analogica della norma penale, attribuire precisa collocazione nell'ambito del codice penale alle varie situazioni riscontrabili.
- Il problema non era nuovo e si era presentato in tema di tutela del software nell'ambito della Legge sul Diritto di Autore, che, in assenza della specifica Legge (la L. n. 518 varata finalmente nel 1992) poteva applicarsi per riconoscimento pressochè costante, dopo qualche tentennamento iniziale, della dottrina e giurisprudenza, ma che non si riteneva pacificamente applicabile per quanto concerneva le norme di carattere penale insite nella L.633/41.

REATI INFORMATICI

- Art. 491 bis c.p.

“ 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. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli”.

REATI INFORMATICI

- Ora, poichè l'atto pubblico, per sua natura, produce effetti costitutivi, traslativi, dispositivi, modificativi ed estintivi, rispetto a situazioni soggettive di rilevanza pubblica, si comprende benissimo l'impegno del legislatore a tutelare la veridicità e l'integrità originale del documento stesso.
- L'elemento soggettivo è quindi offerto dal dolo di violare il principio della pubblica fede, e riteniamo che si dovrà accertare di volta in volta se sussista un'incidenza specifica di dolo o meno (vedasi ad esempio gli artt. 482 e 485 c.p., che contemplano, rispettivamente, “La falsità materiale commessa dal privato" per la quale il dolo è generico, e "La falsità in scrittura privata" per la quale il dolo è specifico) .

REATI INFORMATICI

- **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, è punito con la reclusione fino a tre anni.
- La pena è della reclusione da uno a cinque 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.

REATI INFORMATICI

- **615quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.**
- Chiunque, al fine di procurare a sé 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 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.

REATI INFORMATICI

- **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, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329.

REATI INFORMATICI

- In considerazione della stretta relazione corrente fra le due fattispecie contemplate dagli art. 615 ter ,quater e quinquies, procederemo al loro esame congiuntamente .
- L'art. 615 ter punisce l'accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza o si trattiene , mantenendo il detto accesso contro la volontà di chi abbia diritto di escluderlo.
- Sono stati stabiliti incrementi di pena , portando la reclusione dal massimo di uno, come stabilito nel primo comma, al massimo di cinque anni se il fatto sia commesso da un pubblico ufficiale o incaricato di un pubblico servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato , o con abuso della qualità di operatore del sistema.
- La stessa aggravante di pena ricorre anche nell'ipotesi in cui il colpevole, nel perpetrare il crimine usi violenza sulle cose o alle persone o se sia palesemente armato.
- Alla stessa pena soggiace chi , a seguito dell'accesso abusivo, abbia causato la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, o la distruzione di dati, informazioni o programmi contenuti nel sistema.
- Il legislatore ha stabilito poi un'ulteriore aggravante qualora i fatti riguardino sistemi informatici i 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.

REATI INFORMATICI

- La norma di cui al successivo art. 615 quater tutela la diffusione o la ricerca a buon fine, e ciò, come meglio vedremo, in senso lato, di codici o parole chiave di accesso o altri mezzi idonei all'accesso al sistema fornito i misure di sicurezza, o fornisca informazioni idonee allo scopo sopracitato.
- L'art. 615 quinquies si rivolge alla tutela nei confronti di chi metta in circolazione un programma informatico, proprio o di terzi, idoneo al danneggiamento di un sistema informatico o telematico, dati o programmi compresi o d esso pertinenti, o idoneo a creare interruzione totale o parziale del sistema o la sua alterazione .
- I tre articoli apportano finalmente un preciso contributo alla difesa contro uno dei comportamenti illegittimi e maggiormente diffusi del mondo delle comunicazioni informatiche.

REATI INFORMATICI

- **L'elemento oggettivo è, a nostro giudizio, costituito dal comportamento di accesso "indiscreto", ma a condizione che il sistema goda di misure di sicurezza.**
- **Una prima valutazione dovrà farsi in relazione all'intrusione: ossia 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.**
- **A nostro avviso il semplice fatto che sussistano regole aziendali note, come nell'ipotesi limite ma auspicabile di affissione nella bacheca aziendale di un richiamo alla inviolabilità dei sistemi informativi, o la presenza di chiavi di accesso e di sistemi di sicurezza (elemento fondamentale su cui ci soffermeremo in seguito), identifica la volontà del titolare del diritto al rispetto delle norme.**

REATI INFORMATICI

- **Parallelamente all'accesso palesemente contro la volontà del dominus, riteniamo debba essere considerato , l'accesso che si protenda oltre quanto autorizzato, e così dunque , come nell'ipotesi di un soggetto autorizzato ad accedere e permanere sulla rete per un certo periodo e per specifiche operazioni o solo per specifiche operazioni, con comportamento di questo soggetto che si collochi oltre e contro detta autorizzazione (molto opportunamente il legislatore ha sanzionato sia l'introduzione che il permanere nel sistema, contro la volontà espressa o tacita di chi goda del diritto di escluderlo).**
- **Argomento che offrirà spunto agli operatori del diritto sarà anche quello relativo alla distinzione fra "dissenso tacito" e "dissenso presunto" sottolineandosi come i due concetti possano rendere arduo nella pratica una loro distinta applicazione, nonostante che essi differiscano in quanto il primo "postula una manifestazione ostativa di volontà, percepita come tale dall'agente, mentre il secondo ne prescinde" con la conseguenza che "il dissenso presunto non possa ritenersi sufficiente per l'esistenza del reato".**

REATI INFORMATICI

- Resta infine da determinare chi abbia il diritto di "escludere" l'intruso: riteniamo che tale diritto sia in capo tanto al proprietario della linea, del sistema, dei dati ecc. quanto a chi ne abbia la detenzione o il possesso, come nell'ipotesi di chi stia , ad esempio, utilizzando il sistema non proprio per un service o stia operando in qualità di licenziatario.
- Dalla lettura del testo dell'art. 615 ter c.p. emerge un ulteriore dato meritevole di riflessione: è il riferimento alla necessaria “protezione" del sistema.
- L'attenzione deve quindi accentrarsi sul termine “misura di sicurezza" posto dal legislatore quale elemento condizionante dell'applicabilità della norma: indubbiamente si è voluto porre un onere a carico delle parti e tale onere consiste nell'aver adottato una qualche misura di sicurezza.
- Tale condizione ricorre anche nel successivo articolo, ribadendosi così la necessità di cooperazione “preventiva" da parte del potenziale soggetto passivo del reato.

REATI INFORMATICI

- A sua volta l'Art. 615 quinquies combatte la diffusione, in senso ampio, di programmi atti a danneggiare o interrompere un sistema informatico, così come dimostrato dell'esaustiva elencazione delle fattispecie, elencazione calzante per ogni situazione illegittima, e tutela anch'esso il diritto all'inviolabilità della sfera di interesse economico-sociale introdotta dai precedenti articoli, senza tuttavia richiedere il dolo specifico necessario per l'attuazione della fattispecie dell'art. 615 quater, e così dunque solo implicando “dolo generico", realizzandosi il fatto delittuoso con il semplice crearsi o distribuirsi del prodotto “atto a danneggiare", senza la necessità dell'attuarsi del danno, totale o parziale, o dell'interruzione, ma è sufficiente l'esistenza del prodotto illegittimo.
- Riteniamo interessante anche il raffronto con le disposizioni degli artt. 8 e 10 Legge 518/92 sulla tutela del software, nella parte in cui si riferiscono a mezzi di rimozione fraudolenta dei sistemi di sicurezza.

REATI INFORMATICI

- **616. Violazione, sottrazione e soppressione di corrispondenza**.
- Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, 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
-

REATI INFORMATICI

- Esaminiamo preliminarmente la collocazione della norma nell'ambito dei delitti contro l'inviolabilità dei segreti.
- Con il termine di "segreto" si può intendere qualsiasi informazione o notizia che, nella diversità delle situazioni contemplate dal codice penale, goda di specifica tutela nei confronti di chi voglia rendere nota la notizia al di fuori dell'effettivo titolare del diritto di escludere altri dalla divulgazione.
- La dottrina ha ravvisato tale diritto o nella potestà dello Stato o in un diritto della personalità o, infine, in un diritto di proprietà.
- A questi requisiti debbono aggiungersi i due ulteriori aspetti della riservatezza delle informazioni e dell'interesse “giuridicamente apprezzabile a che la loro conoscenza non venga conseguita, divulgata o utilizzata senza il suo consenso"

REATI INFORMATICI

- L'art. 614 c.p. con il suo quarto comma garantisce la libertà di qualsiasi forma di comunicazione, e così dunque anche a sistemi del tutto particolari come quelli attuati tramite INTERNET, su cui torneremo brevemente in seguito, e conseguentemente protegge il diritto di celare a terzi il contenuto delle comunicazioni.
- La punibilità è legata alla presa di “cognizione" del contenuto di corrispondenza, non implica necessariamente la lettura, ma sarebbe sufficiente la conoscenza del contenuto : così la Cassazione aveva ritenuto applicabile l'art. 616 c.p. per il semplice fatto di “sapere che taluno ha inviato ad altri del denaro costituisce cognizione dell'oggetto della corrispondenza, indipendentemente dal fatto che la busta contenga o meno una missiva di accompagnamento."
- Conseguentemente avremo una estensione indubitabile della fattispecie criminosa, ma è altrettanto vero che si potrà discutere a lungo sui presupposti riportati nel primo comma: ".. corrispondenza chiusa a lui non diretta ovvero...una corrispondenza chiusa o aperta, a lui non diretta..".

REATI INFORMATICI

- **617quater. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.**
- **Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la 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.**

REATI INFORMATICI

- **617quinquies. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.**
- Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito 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.

REATI INFORMATICI

- **617sexies. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.**
- Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, 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, 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.

REATI INFORMATICI

- L'articolo 617 quater tutela la libertà di circolazione delle informazioni attraverso i nuovi sistemi di trasmissione informatici e telematici e quindi alla loro intercettazione , impedimento o interruzione : quindi la massima tutela per quanto concerne il diritto di “movimento" delle informazioni.
- 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.
- Mentre i soggetti sono di due tipi distinti: chi interviene e chi diffonde, rivelandole in qualsiasi modo, le informazioni.
- Le aggravanti sono indicate nel testo di articolo.

REATI INFORMATICI

- **Il successivo articolo, il 617 quinquies, tutela sempre la libertà e riservatezza delle informazioni, contrastando l'attività di coloro che installano le apparecchiature atte a intercettare, impedire o interrompere le comunicazioni: che poi dette apparecchiature funzionino o meno è ininfluente, ciò che rileva è il semplice fatto della loro installazione al di fuori dei casi consentiti.**
- **Il dolo è specifico ed offerto dalla volontà di installare allo scopo di perseguire l'intercettazione, l'impedimento o la interruzione: dovrebbe quindi essere esclusa l'installazione per studio, ricerca, gioco e svago, benchè ci paia che tale esclusione non possa essere ammissibile.**
- **L'art. 617 sexies tutela l'integrità, la veridicità, la genuinità, la sicurezza delle informazioni, e pertanto l'elemento oggettivo è offerto dalla formazione, modificazione o soppressione totale o parziale del contenuto della comunicazione ,in qualunque modo avvenga purchè 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.**

REATI INFORMATICI

- **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.

REATI INFORMATICI

- **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.

REATI INFORMATICI

- Procediamo all'esame dei due articoli nell'ambito dello stesso contesto in quanto entrambi mirati a tutelare la inviolabilità dei segreti.
- La novità relativa al testo dell’art. 621 c.p. è inserita nell'ultimo comma ove, espressamente, si estende 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".
- Infatti , la norma , integrando quanto precedentemente disposto in tema di segreto di corrispondenza, chiude, per così dire , lo spazio di ingerenza di terzi a qualsiasi dato inserito o riportato da supporto informatico, che, al limite contenga anche solo un programma software.

REATI INFORMATICI

- 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.
- L'art. 623 bis. c.p. 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".
- Ne consegue che l'elemento oggettivo sarebbe il medesimo di cui all'art. 617 c.p. e ss. e così la cognizione, interruzione o impedimento, con il relativo dolo specifico.
- E' stato asserito che l'articolo in esame "intende soprattutto direttamente riferirsi agli artt. 622 e 623 c.p. e cioè alle ipotesi di rivelazione del segreto professionale e di rivelazione di segreti scientifici o industriali : uniche ipotesi che non vengono considerate espressamente da prescrizioni modificative o integrative della nuova legge"
- A nostro giudizio il riferimento dell'art. 623 bis. è nel senso più ampio, e quindi estensibile a tutte le fattispecie relative alla inviolabilità dei segreti.

REATI INFORMATICI

Art.635 bis- Danneggiamento di sistemi informatici e telematici

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 reclusuione 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 reclsuione da uno a quattro anni.

REATI INFORMATICI

- **Con l'introduzione del presente articolo si tutela pienamente l'integrità dei beni e del patrimonio, superando ed eliminando qualsiasi precedente dubbio interpretativo originato dalla immaterialità del bene informatico.**
- **Richiamiamo quanto scritto nelle pagine precedenti in ordine ai “reati informatici" prima dell'introduzione della legge 547/93, con particolare riferimento alla difficoltà di collegare il reato di danneggiamento al concetto informatico. Il danno deve essere tale da integrare una pur minima modifica strutturale o funzionale del bene o implicarne un pur minimo deterioramento.**
- **Riteniamo che, proprio per la particolare natura del bene informatico, si debba considerare quest'ultimo, con maggior attenzione rispetto a qualsiasi altro bene mobile.**
- **E basti, infine, riflettere su quanto detto e scritto e “patito” da molti utenti in tema di Virus Informatici.**
- **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.**

REATI INFORMATICI

- **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 .

REATI INFORMATICI

- L'interesse tutelato dall'articolo in esame si identifica, da un lato, nel bene inteso come patrimonio-prodotto, e dall'altro, nella buona fede.
- E' indubitabile che l'inserimento del nuovo articolo, dopo la precedente estensione attivata con l'introduzione dell'art. 640 bis (truffa aggravata per il conseguimento di erogazioni pubbliche), accentri l'attenzione sul settore informatico e telematico.
- 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.
- Siamo pertanto in presenza del consolidato principio dottrinale e giurisprudenziale di ammissibilità dell'ampliamento dei limiti originariamente tracciati dall'art. 640 c.p..

REATI INFORMATICI

- Va notato come il legislatore non abbia richiamato nell'articolo in esame, gli “artifici e raggiri" ponendo un collegamento con la disposizione del capo II, “dei delitti contro l'industria ed il commercio" e la truffa vera e propria.
- 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).
- L'articolo richiama inoltre le aggravanti proprie dell'art. 640 c.p..

REATI INFORMATICI

- ***RIFLESSIONI SU ALCUNE SPECIFICHE FORME DI CRIMINALITA' IN INTERNET***
- In ambito INTERNET la valutazione delle possibili fattispecie criminali può assumere diversa angolazione.
- In particolare si possono distinguere attività criminali poste in essere senza il concorso di terze persone o con il concorso , materiale o, se ne ricorrano i presupposti, morale.
- Altra peculiarità è offerta dalla natura dei crimini presi in esame.
- Si potranno così avere :
- attività criminali dirette contro i sistemi telematici
- attività criminali poste in essere attraverso i sistemi telematici
- attività criminali dirette contro i sistemi telematici e con sistemi telematici.

REATI INFORMATICI

- 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.

REATI INFORMATICI

- Con l'impatto di INTERNET tali figure criminali assumono nuova portata e devono essere inquadrate nel nuovo contesto,con la necessaria ricerca del presupposto attuativo: un esempio può essere offerto dall'art. 594 c.p. italiano che contempla il reato di *ingiuria "chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa sino a lire un milione.*
- *Alla stessa pena è soggetto chi commette il fatto mediante comunicazione telegrafica o telefonica,o con scritti e disegni, diretti alla persona offesa.*
- *La pena è della reclusione fino ad un anno o della multa fino a lire due milioni, se l'offesa consiste nell'attribuzione di un fatto determinato.*
- *Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone.".*

REATI INFORMATICI

- **600 ter c.p. (*Pornografia minorile)* : "*Chiunque sfrutta minori degli anni diciotto alò fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la 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.***
- ***Chiunque , al di fuori delle ipotesi di cui al primo e secondo comma, 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, è punito con la reclusione da uno a cinque anni e con la multa da € 2.582 a €.51.645.***
- ***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 ani diciotto, è punito con la reclusione fino a tre anni o con la multa da € 1.549 a € 5.164."***

REATI INFORMATICI

- L'art. 600 quater c.p. (*Detenzione di materiale pornografico)* così recita : "*Chiunque, al di fuori delle ipotesi previste nell'art. 600 ter, consapevolmente , procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale di minori degli anni diciotto è punito con la reclusione fino a tre anni o con la multa non inferiore a€ 1.549.".*
- L'art. 600 quinquies c.p. *(Iniziative turistiche volte allo sfruttamento della prostituzione minorile)* così recita : "*Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione in danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da € 15.493 a € 154.937".*

REATI INFORMATICI

l'art. 604 c.p. (*Fatto commesso all'estero) che così recita : " 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.".*

REATI INFORMATICI

- resta evidente il problema del *LOCUS COMMISSI DELICTI*, giacchè una delle peculiarità di INTERNET è proprio quella della impossibilità della delimitazione territoriale sia per quanto concerne l'immissione dei dati, la loro disponibilità ed accessibilità.
- Non esiste più quello che tradizionalmente viene identificato come lo spazio nazionale: si opera in un diverso spazio (cyber spazio) che va ben al di là delle frontiere riconosciute dal diritto interno ed internazionale.
- Nel cyber spazio possono essere presi in considerazione diversi parametri e quindi ritenere preponderante o il luogo di immissione dei dati o il luogo di ricezione dei dati.

REATI INFORMATICI

- Fra le due, la prima scelta ci appare di maggior consistenza in quanto consente la determinazione precisa del fatto con riferimento al momento attuativo dell'azione , evitando così conflitti fra normative che potrebbero essere profondamente divergenti: basti a tal fine esaminare le diverse concezioni che esistono in ordine ad un determinato fatto in un Paese di influenza religiosa diversa da un altro di diversa influenza religiosa o di interpretazione meno rigorosa: una medesima comunicazione potrebbe costituire fatto penalmente rilevante in uno Stato e non in un altro.

REATI INFORMATICI

- Ma è altrettanto vero che si potrebbe accedere ad una terza via, quella della così detta "*ubiquità",* che considera parimenti sia il luogo ove nasce l' *azione* , sia il luogo ove si verifica l'*evento*: e tale estensione implica anche l'allargamento del concetto di *azione* all'intero ciclo di comunicazione dell'informazione, e quindi con possibile ricomprensione , ove ne ricorrano i presupposti, della responsabilità anche del Provider.
- Alla luce di tali osservazioni appare positiva la formulazione della norma penale così come riportata nei sopracitati articoli contro la Pornografia Minorile.
- In ogni caso un giudicato della cassazione penale, depositata il 27 dicembre 2000 n. 4741 ha riconosciuto la competenza del giudice italiano in presenza di diffamazione on line attuata attraverso immagini o frasi lesive della dignità di un cittadino italiano immesse in un Web all'estero.

REATI INFORMATICI

- Il principio ora sancito ribalta la precedente posizione che , considerando la diffamazione un reato di condotta, ne collocava il perfezionamento nel paese in cui si attuava l'immissione in rete: con il giudicato in esame, la cassazione ha definito la diffamazione on line un reato di evento e non più di condotta , ritenendo di essere, nel caso specifico, in presenza di un evento psicologico che consiste nella percezione da parte del terzo leso della espressione offensiva.
- Conseguentemente il momento perfezionativo del reato si avrà non all'atto dell'immissione e diffusione del messaggio, ma nel momento in cui il messaggio stesso viene percepito, applicandosi così l'art. 6 c.p. comma secondo, applicandosi anche per la diffamazione la teoria dell'ubiquità.

REATI INFORMATICI

- Ma vi è un ulteriore interessante aspetto di rapporti fra norma penale e Internet, e ci riferiamo alla possibilità di acquisto via Internet di prodotti o sostanze non consentite dalla legge, siano essi carri armati, gas nervini o, più semplicemente, ma non meno dirompentemente, sostanze stupefacenti o assimilate.
- E', in altre parole, il principio di applicazione del **D.P.R. 9 ottobre 1990 n. 309 " Testo Unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione , cura e riabilitazione dei relativi stati di tossicodipendenza ".**

REATI INFORMATICI

- Fin qui nulla di strano, la legge esiste e deve essere rispettata.
- Qualche riflessione deve essere però fatta in ordine ad un particolare mezzo di distribuzione dei prodotti: cioè relativamente alla possibilità di acquisto, ad esempio, di medicinali via Internet.
- Poiché la legge proibisce il commercio (in senso più che ampio) dei prodotti ritenuti stupefacenti o psicotropi, è evidente che il problema pratico si ponga.
- Preliminarmente occorre valutare il “mezzo” , cioè Internet.

REATI INFORMATICI

- Nel caso in esame Internet non si pone come lo “strumento diretto” per l’attuazione del fatto criminoso, così come sarebbe nell’ipotesi di duplicazione di software o di file musicali, bensì opera alla stregua di un comune mezzo di comunicazione, quale potrebbe essere il telefono.
- Ciò non esclude però la fattispecie criminosa, ma, anzi, ne costituisce una delle modalità strumentali di attuazione.

REATI INFORMATICI

- Altra distinzione da farsi è quella relativa ai vari soggetti interessati all'intera operazione, accentrando ovviamente l'attenzione su prodotti farmaceutici rientranti nella categoria disciplinata dalla legge e quindi con esclusione, nell'asame in corso dei " classici " stupefacenti (cocaina, eroina, droghe sintetiche, ecc...), e tali soggetti sono:
- il fabbricante
- il gestore del sito
- il provider
- l'utente finale ordinante per ridistribuirlo
- l'utente finale per acquisto proprio

REATI INFORMATICI

- 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 fabricante, 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.

REATI INFORMATICI

- In caso contrario potrà concorrere con altri soggetti nella perpetuazione del delitto e quindi aggravare pesantemente la sua, e degli altri, posizione , facendo scattare l'ipotesi di cui all'art. 74 d.p.r. 309/99 modificato dalla L-26.6.1990 n. 162 artt.14,comma 1 e 38 comma 2, *associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope,* che al primo comma recita: " *Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'art. 73, chi promuove,costituisce, dirige, organizza o finanzia l'associazione, è punito per ciò solo con la reclusione non inferiore a venti anni."*
- Basta tale letura per rendersi conto della gravità della fattispecie.

REATI INFORMATICI

- La legge 62/2001 estende una serie di norme penali, sia direttamente esposte sia richiamate dalle precedenti leggi (n.416/1981 e n. 47/1948) ai “ prodotti editoriali” e quindi , al di là delle sanzioni legate all’omessa registrazione delle imprese editrici, resta il principio della diffamzione a mezzo stampa e delle fattispecie contemplate dagli artt. 11,12,13,14 ,15,16,17,18,19,20 e 21 della legge 47/1948.
- A questo punto si ritornerebbe, soprattutto per l’ipotesi di diffamazione, nell’ottica dei giudicati anteriori all’ Ordinanza del Tribunale di Roma del 22 marzo 1999, e quindi alla ricomprensione della rete Internet nell’ambito degli strumenti editoriali, riaprendo così i termini della questione anche per il Provider, che potrebbe essere equiparato ad un editore o ad uno stampatore, con tutte le ovvie conseguenze.

REATI INFORMATICI

- E, necessariamente la sede dell'Hosting o dell'Hausing diventerebbe la sede editoriale utile ai fini della registrazione, con l'ulteriore evidente difficoltà interpretativa e attuattiva nell'ipotesi di sito situato all'estero e dal quale giungano in Italia le informazioni.
- Pertanto anche a fronte di queste brevi riflessioni in materia penale può quindi rilevarsi come la novità della materia (l'utilizzo dello strumento Internet) offra precisi e urgenti motivi di approfondimento nell'area del diritto penale oltrecchè del diritto civile.