La funzione del diritto penale e della pena

Una definizione di diritto…

- Disciplina coattiva della vita sociale
- Norma giuridica:
  - Descrizione di un fatto giuridicamente rilevante;
  - Conseguenza giuridica relativa a quel fatto.

… e di diritto penale

PENA = particolare tipo di conseguenza giuridica

- **Afflittività**: la pena colpisce beni rilevanti (libertà personale, patrimonio)
- **Inidoneità ad eliminare le conseguenze dannose del reato** (diversamente la sanzione civile)

Le funzioni della pena

- **Funzione retributiva:** si punisce per il solo fatto di aver commesso un reato
- **Funzione preventiva:** si punisce per evitare la commissione di ulteriori illeciti
  - Prevenzione generale
  - Prevenzione speciale

Le caratteristiche della pena

- **Umanità**
  - *"Le pene non possono consistere in trattamenti contrari al senso di umanità" – Art. 27, III co., Cost.*
- **Proporzionalità**
  - La pena deve essere proporzionata all'offesa arrecata al bene giuridico tutelato
- **Rieducazione**
  - *"Le pene […] devono tendere alla rieducazione del condannato" – Art. 27, III co., Cost.*

Il catalogo delle pene (art. 17 c.p.)

- **Delitti** (reati di maggiore gravità)
  - Ergastolo *(pena detentiva a vita)*
  - Reclusione *(pena detentiva)*
  - Multa *(pena pecuniaria)*
- **Contravvenzioni** (reati di minore gravità)
  - Arresto *(pena detentiva)*
  - Ammenda *(pena pecuniaria)*

Il sistema delle garanzie

Il principio di legalità ed i suoi corollari

Il sistema delle garanzie

- Principio di legalità (Art. 25, II co., Cost.)
- Principio di irretroattività (Art. 25, II co., Cost.)
- Principio di colpevolezza (Art. 27, I co., Cost.)

Il principio di legalità

- Art. 25, II comma, Cost. *"Nessuno può essere punito se non **in forza di una legge**"*
- Art. 1 c.p. *"Nessuno può essere punito per un fatto che non sia espressamente preveduto come reato **dalla legge**, né con pene che non siano da essa stabilite"*

1. La riserva di legge

Il catalogo delle fonti del diritto

Fonti superprimarie

- Costituzione, Leggi di revisione costituzionale e Leggi costituzionali

Fonti primarie

- Legge dello Stato
- Atti aventi forza di Legge (decreti legge e decreti legislativi)
- Legge regionale
- Normativa di fonte europea e comunitaria

Fonti secondarie

- Regolamenti (statali, regionali, territoriali)

Fonti fatto

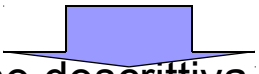
- Usi e consuetudine

…segue

- Riserva di legge **assoluta**
- Riserva di legge **relativa**
- Riserva di legge **tendenzialmente assoluta**: *la fattispecie è interamente individuata dalla norma ma è ammesso il richiamo alla fonte secondaria per specificare il precetto*

2. Il principio di precisione

Certezza del precetto



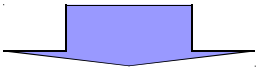
Formulazione descrittiva del precetto

(chiarezza ed inequivocità)

È possibile ricondurre il caso concreto alla fattispecie astratta prevista nel precetto

3. Il principio di determinatezza

Il precetto penale deve riferirsi a fenomeni che **possano realizzarsi**



La possibilità di realizzazione deve essere concretamente **verificabile**

4. Il principio di tassatività

Il divieto di analogia in *malam partem*

- Divieto di estendere l'ambito di applicabilità della norma incriminatrice ai casi non espressamente previsti
  - nei confronti del legislatore
  - nei confronti del giudice

Il sistema delle garanzie

Il principio di irretroattività

Il principio di colpevolezza

Irretroattività della legge penale

Art. 2, comma I, c.p.

"Nessuno può essere punito per un fatto che, secondo la legge del tempo in cui fu commesso, non costituiva reato"

Retroattività in *bonam partem*

È ammessa l'applicazione retroattiva se si concreta in un trattamento favorevole per il reo

Fondamento costituzionale:

Principio di uguaglianza (art. 3 Cost.)

Inopportunità di punire in modo diverso reati "uguali", solo perché commessi in tempi diversi

Ipotesi di Iperretroattività

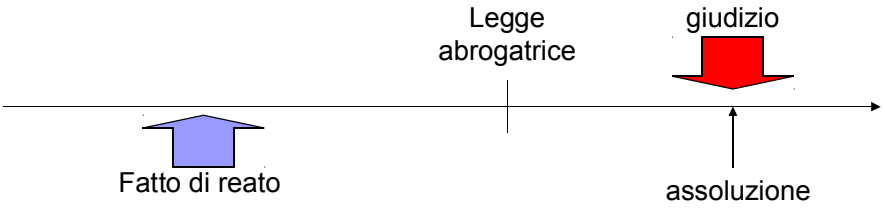
Abolitio criminis e *conversione in pena pecuniaria*

- ***Abolitio criminis*:** il fatto illecito diviene, in forza di una legge successiva, lecito. (art. 2, II comma, c.p.)
- **Conversione in pena pecuniaria:** il fatto, punito con una pena detentiva, viene punito, in forza di legge successiva, con la sola pena pecuniaria. (art. 2, III comma, c.p.)

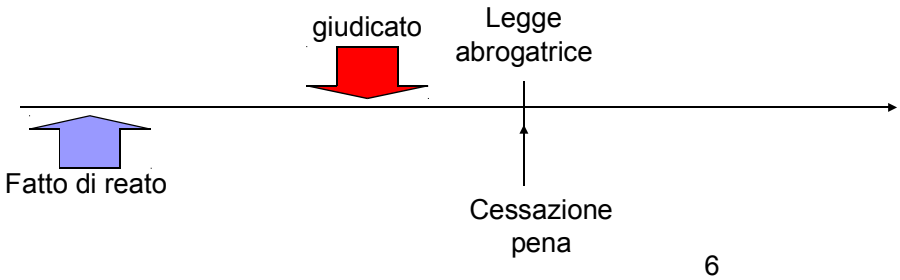
…segue: gli effetti

1. Se non è intervenuta sentenza passata in giudicato:
   a. assoluzione
   b. o condanna a pena pecuniaria
1. Se è intervenuta sentenza passata in giudicato:
   a. cessa l'esecuzione della pena e gli effetti penali o
   b. si converte il residuo in pena pecuniaria)

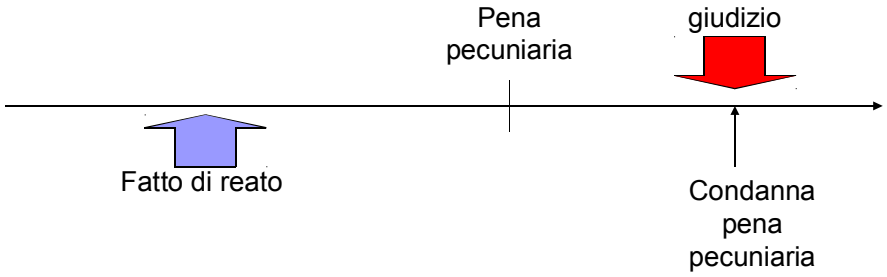
1.a.



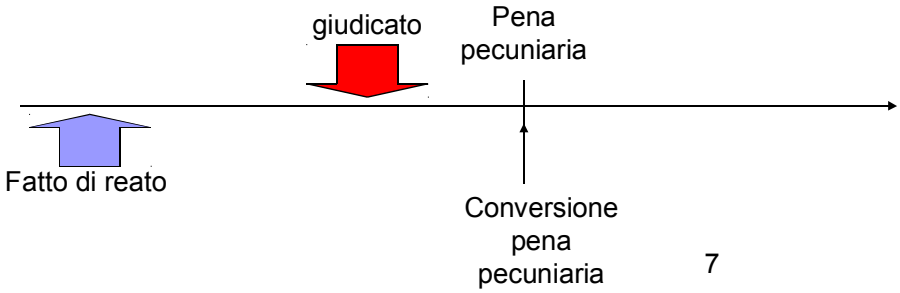
1.b.



2.a.



2.b.



Successione di leggi

Il *favor rei*

Caso in cui nel tempo si succedano due leggi:

1. Se non è intervenuta sentenza passata in giudicato

   ⇓

   Si applica la **legge più favorevole** al reo

2. Se è intervenuta sentenza passata in giudicato

   ⇓

   Si applica la **legge del tempo** in cui fu commesso il fatto

Principio di colpevolezza

Fondamento costituzionale

Art. 27, I comma, Cost.

“La responsabilità penale è personale”

La struttura del reato: il fatto

La struttura del reato

- Fatto tipico
- Antigiuridicità
- Colpevolezza

Il fatto: nozione

Insieme degli elementi oggettivi che individuano e caratterizzano ogni singolo reato come specifica forma di offesa ad uno o più beni giuridici

Gli elementi del fatto

- I presupposti della condotta
- La condotta (commissiva od omissiva)
- L'evento
- Il nesso di causalità tra condotta ed evento
- L'oggetto materiale

Reati comuni e reati propri

A seconda del soggetto attivo individuato dalla norma

- **Reati propri:** reati che possono essere solo da soggetti aventi una particolare qualifica
- **Reati comuni:** reati che possono essere commessi da chiunque

Reati a forma libera e reati a forma vincolata

A seconda del grado di descrittività della condotta nella norma

- **Reati a forma libera:** la norma non contiene una descrizione delle modalità con cui si deve realizzare l'offesa
- **Reati a forma vincolata:** la norma descrive puntualmente le modalità con cui si deve realizzare l'offesa

Reati di condotta e reati di evento

A seconda che la norma richieda o meno il verificarsi di un evento

- **Reati di mera condotta:** la semplice commissione dell'azione vietata importa la responsabilità penale
- **Reati di evento:** l'azione deve causare il verificarsi di un evento (tipizzato)

Reati commissivi e reati omissivi

- A seconda delle modalità di realizzazione della condotta
- **Reati commissivi:** la condotta consiste in un azione dell'agente
- **Reati omissivi:** la condotta consiste nell'inerzia dell'agente

I reati commissivi impropri

Reati omissivi propri e reati omissivi impropri

- **Reati omissivi propri:** è punito il mancato compimento dell'azione che il precetto comanda
- **Reati omissivi impropri:** è punito il mancato impedimento di un evento che si aveva l'obbligo giuridico di impedire (art. 40, II comma, c.p.)

Le posizioni di garanzia nei reati omissivi impropri

- **Posizioni di protezione:** particolare legame giuridico tra il garante ed i beni
- **Posizioni di controllo:** dominio sulla fonte del pericolo

L'obbligo di impedire l'evento

I presupposti

- Preesistenza di poteri giuridici di impedire l'evento
- Possibilità materiale di impedire l'evento
- Effettiva presa in carico del bene giuridico tutelato

L’obbligo di impedire l’evento

Le fonti

- Fonti normative (di qualsiasi genere)
- Fonti convenzionali (contratti o atti unilaterali)
- Contatto sociale (affidamento)
- Assunzione volontaria dell’obbligo giuridico (solo se l’assunzione determina un aumento del rischio)

Il problema della causalità

Il problema della causalità

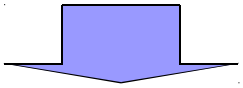
Art. 40, I comma, c.p.

"Nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso da cui dipende l'esistenza del reato, non è conseguenza della sua azione od omissione"

Pluralità di cause

Art. 41, comma I, c.p.

Anche se esistono più cause che, congiuntamente, hanno contribuito a causare l'evento



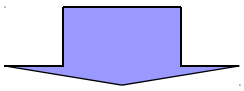
Il rapporto di causalità rispetto alla condotta **non è escluso**

La *conditio sine qua non*

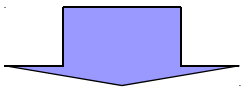
Sussiste il rapporto di causalità nel caso in cui la condotta dell'agente sia **condizione necessaria** (anche se non sufficiente) al verificarsi dell'evento

Il procedimento di eliminazione mentale

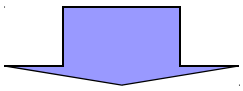
Si procede all'**eliminazione mentale della condotta dell'agente**



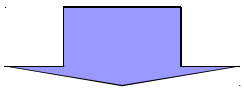
Se l'evento si sarebbe comunque verificato



Il nesso causale **non sussiste**



Se l'evento non si sarebbe verificato



Il nesso causale **sussiste**

La sussunzione sotto leggi scientifiche

- Leggi scientifiche universali e corroborate
- Leggi statistiche
- Leggi probabilistiche (?)

Le serie causali atipiche

Art. 41, comma II, c.p.

Le cause sopravvenute escludono il rapporto di causalità quando sono da sole sufficienti a cagionare l'evento

I reati di pericolo

Reati di pericolo

il fatto tipico consiste in una **condotta** o nella **causazione di un evento pericolosi**, poiché probabili cause del verificarsi di una lesione al bene giuridico protetto

Tipologie di reati di pericolo

In base alla formulazione della fattispecie, si può distinguere tra:

- **reati di pericolo concreto**
  - Il giudice accerta che il fatto sia in concreto pericoloso
- **reati di pericolo astratto**
  - Il legislatore stabilisce a monte la pericolosità del fatto tipico

Reati di pericolo concreto

- Il pericolo costituisce un **elemento essenziale** della fattispecie
- viene **esplicitato** nella descrizione del fatto

Es.: **Art. 450. Delitti colposi di pericolo.** Chiunque, con la propria azione od omissione colposa, fa sorgere o persistere il pericolo di un disastro ferroviario, di una inondazione, di un naufragio, o della sommersione di una nave o di un altro edificio natante

Reati di pericolo astratto

- Il fatto descritto nella norma incriminatrice costituisce una **tipica fonte di pericolo** per il bene giuridico tutelato

Es.: **Art. 443. Commercio di medicinali guasti.** Chiunque detiene per il commercio, pone in commercio o somministra medicinali guasti o imperfetti, è punito con la reclusione da 6 mesi a 3 anni e con la multa non inferiore a euro 103".

Reati di pericolo indiretto

Ulteriore anticipazione della tutela al *"pericolo di pericolo"*:

- **Reati di pericolo di un evento pericoloso**
  - Es: art. 423 c.p. delitto di incendio
- **Reati di possesso**
  - Necessariamente indiretti (detenzione di stupefacenti)
  - Eventualmente indiretti (possesso ingiustificato di chiavi alterate e grimaldelli).

La struttura del reato: L'antigiuridicità

L'antigiuridicità

Rapporto di contraddizione tra il fatto tipico e l'intero ordinamento giuridico

Il fatto commesso, astrattamente riconducibile alla norma penale, non deve essere in concreto consentito da altre norme (principio di unità dell'ordinamento giuridico)

La rilevanza oggettiva della giustificazione

Il giudizio di liceità è **oggettivo**, in quanto non dipende dalle valutazioni, dalle conoscenze o dalle finalità del singolo agente

Art. 59 c.p.

le cause di giustificazione "*sono valutate a favore dell'agente* ***anche se da lui non conosciute o da lui per errore ritenute inesistenti***"

Le ragioni della giustificazione

- **Consenso del titolare del diritto offeso**
  - consenso dell'avente diritto
- **Esistenza di una norma nell'ordinamento che consente o impone il fatto**
  - esercizio di un diritto/adempimento di un dovere
- **Reazioni in situazioni 'di necessità'**
  - legittima difesa / stato di necessità / uso legittimo della coazione da parte della forza pubblica

Esercizio di un diritto o adempimento di un dovere

Consenso dell'avente diritto

Esercizio di un diritto e adempimento di un dovere

Art. 51 c.p.

*L'**esercizio di un diritto** o l'**adempimento di un dovere**, imposto da una norma giuridica o da un ordine legittimo della pubblica autorità, esclude la punibilità*

Espressione del principio di non contraddizione

Il consenso dell'avente diritto

Art. 50 c.p.

Non è punibile chi lede o pone in pericolo un diritto, col consenso di chi può validamente disporne

Consenso che rende **lecito** un fatto tipico

Il consenso che esclude la tipicità

Il consenso non è causa di giustificazione

Se la norma incriminatrice prevede il consenso come elemento costitutivo del fatto

Es.: violazione di domicilio, violenza sessuale

I diritti disponibili

- Diritti personali (riservatezza, libertà personale, …)
- Diritti patrimoniali (proprietà, possesso, …)
- Diritto all'integrità fisica, se esercitato nei limiti dell'art. 5 c.c.

I diritti indisponibili

- Interessi dello Stato e di Enti pubblici
- Interessi della famiglia
- Interessi diffusi (o collettivi)
- Diritto alla vita (art. 579 c.p.)

I requisiti del consenso

- **Titolarità** del diritto in capo a chi ne dispone
- **Capacità di intendere e di volere**
- **Assenza di vizi della volontà** (errore, violenza, dolo)
- **Libertà nella forma di espressione**
- **Possibilità di condizioni o termini** (purché esistenti al momento del fatto)
- **Revocabilità**

Legittima difesa

Stato di necessità

La legittima difesa

Art. 52 c.p.

*Non è punibile chi ha commesso il fatto, per esservi stato costretto dalla **necessità** di difendere un diritto proprio od altrui contro il pericolo attuale di una offesa ingiusta, sempre che la difesa sia **proporzionata** all'offesa*

La norma ha la funzione di ammettere, ricorrendone le condizioni, il ricorso all'autotutela (vietato, in via generale*)*

I presupposti della scriminante

- Pericolo **attuale** di un'offesa ingiusta
  - Il pericolo **non** deve essere passato o futuro
  - Il pericolo deve essere tale da non poter attendere la tutela da parte dell'Autorità
- **Necessità** della difesa
  - Mezzo minimo necessario per evitare l'offesa
- **Proporzione** tra offesa e difesa
  - Si valuta mettendo in relazione i beni giuridici

Le aggressioni nei luoghi di privata dimora o di esercizio dell'attività

Art. 52, comma II, c.p.

Nei casi previsti dall'art. 614, I e II comma, ***sussiste il rapporto di proporzione*** […] *se taluno legittimamente presente in uno dei luoghi ivi indicati usa un'arma legittimamente detenuta o altro mezzo idoneo al fine di difendere:*

la propria o la altrui incolumità;

i beni propri o altrui, quando non vi è desistenza e vi è pericolo d'aggressione.

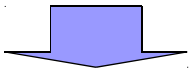
Lo stato di necessità

Art. 54 c.p.

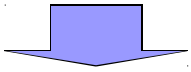
*Non è punibile chi ha commesso il fatto per esservi stato costretto dalla **necessità** di salvare sé od altri dal pericolo attuale di un danno grave alla persona, pericolo da lui non volontariamente causato, né altrimenti evitabile, sempre che il fatto sia proporzionato al pericolo*

Differenze con la legittima difesa

La situazione che minaccia la persona **non** è causata dall'**aggressione** di colui che subisce l'azione difensiva



L'azione colpisce un **terzo innocente**



Il terzo innocente danneggiato ha diritto ad un'indennità (art. 2045 c.c.)

I presupposti della scriminante

- Come per legittima difesa:
  - attualità del pericolo
  - necessità della difesa
  - proporzione tra offesa e pericolo
- In aggiunta:
  - Il pericolo di danno è grave e diretto alla persona
  - Il pericolo non è volontariamente causato
  - Il pericolo non è altrimenti evitabile

La struttura del reato: la colpevolezza

I presupposti della colpevolezza

- **Imputabilità**
  - capacità di intendere e di volere
- **Criteri di imputazione soggettiva**
  - dolo, colpa e preterintenzione

L'imputabilità

Art. 85 cod. pen

*Nessuno può essere punito per un fatto preveduto dalla legge come reato se, al momento in cui lo ha commesso, **non era imputabile**.*

*E' imputabile chi ha la capacità di **intendere** e di **volere**".*

…Segue

- Capacità di intendere: capacità di normale percezione della realtà e di comprensione del significato proprio comportamento
- Capacità di volere: capacità di controllo e di scelta sulle proprie azioni

Vizio di mente

Vizio di mente totale (art. 88 c.p.)

Non è imputabile chi, nel momento in cui ha commesso il fatto era, per infermità, in tale stato di mente da escludere la capacità di intendere e di volere

Vizio di mente parziale (art. 89 c.p.)

Chi, nel momento in cui ha commesso il fatto, era, per infermità, in tale stato di mente da scemare grandemente, senza escluderla, la capacità d'intendere o di volere, risponde del reato commesso; ma la pena è diminuita

La minore età

Art. 97 c.p.

Non è imputabile chi, nel momento in cui ha commesso il fatto, non aveva compiuto i ***quattordici anni***

Art. 98 c.p.

E' imputabile chi, nel momento in cui ha commesso il fatto aveva compiuto i ***quattordici anni*** *ma non ancora i* ***diciotto****, se aveva capacità di intendere e di volere; ma la pena è diminuita*

Ubriachezza

L'imputabilità è esclusa:

- se ubriachezza dovuta a caso fortuito o forza maggiore e tale da escludere totalmente la capacità di intendere e di volere;
- se intossicazione cronica da alcool, tale da escludere totalmente la capacità di intendere e di volere

…Segue

La pena è aumentata:

- se l'ubriachezza è "*preordinata al fine di commettere il reato o di prepararsi una scusa*"
- se l'ubriachezza è abituale

I criteri di imputazione soggettiva

Il dolo e la colpa

I criteri di imputazione soggettiva

Art. 42 c.p.
Distingue tra delitti e contravvenzioni

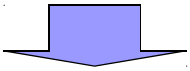
Per i **delitti**:
Nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con ***dolo****, salvi i casi di delitto preterintenzionale o colposo espressamente preveduti dalla legge.*

Per le **contravvenzioni**:
Nelle contravvenzioni ciascuno risponde della propria azione od omissione cosciente e volontaria ***sia essa dolosa o colposa***

La definizione di dolo

Art. 43 c.p.

Il delitto è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente **preveduto e voluto** come conseguenza della propria azione od omissione".



Forma **più grave** di colpevolezza

Gli elementi del dolo

Rappresentazione

Tutti gli elementi che caratterizzano la fattispecie concreta devono costituire **oggetto di rappresentazione da parte dell'agente**

Es.: nella truffa, l'agente si deve rappresentare di porre in essere una serie di condotte artificiose che, inducendo un soggetto in errore, lo inducano a compiere un atto di disposizione patrimoniale, a proprio danno e a favore dell'agente o di un terzo.

Volontà

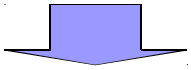
L'agente deve mostrare la **volontà di realizzare il fatto costituente reato**

Forme di dolo

- **Dolo intenzionale**
  - L'agente ha di mira la realizzazione del fatto
  - Premeditazione (circostanza aggravante)
- **Dolo diretto**
  - L'agente si rappresenta la realizzazione del fatto di reato in termini di certezza
  - es.: incendio la casa che so essere abitata per riscuotere il premio dell'assicurazione
- **Dolo eventuale**
  - L'agente si rappresenta la possibilità che si realizzi il reato e sceglie di agire lo stesso, anche a costo di realizzarlo

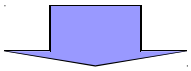
Dolo generico e specifico

Dolo generico



Consiste nella rappresentazione e volizione di tutti gli elementi del fatto di reato

Dolo specifico



Il dolo dell' agente ha una finalità ulteriore, estranea al fatto di reato, alla quale viene dato rilievo soggettivo

Il dolo nei reati omissivi

Reati omissivi propri

- conoscenza della situazione tipica
- consapevolezza e volontà di non compiere un'azione rappresentata come possibile

Reati omissivi impropri

- conoscenza della situazione tipica e volontà di non impedire l'evento con un'azione rappresentata come possibile
- conoscenza degli elementi dai quali deriva la posizione di garante

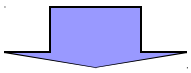
La definizione di colpa

Art. 43 c.p.

Il delitto è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di ***negligenza o imprudenza o imperizia*** *ovvero per* ***inosservanza di leggi, regolamenti, ordini e discipline***

Colpa generica

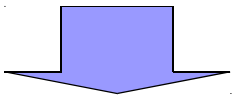
Le regole cautelari non sono formalizzate



- Ricostruzione delle regole cautelari rilevanti
  - Prevedibilità
  - Evitabilità
- Parametro dell'**agente ideale** nell'abito della stessa attività nell'esercizio della quale è stato commesso il reato

Colpa specifica

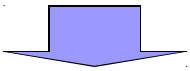
Cambia la fonte della regola, il cui contenuto cautelare resta però invariato



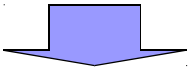
Le regole cautelari sono **formalizzate** in "leggi, regolamenti, ordini o discipline"

Il nesso tra colpa e evento

Affinché sia integrata la colpa deve sussistere un **nesso causale** tra l'evento e l'inosservanza della regola cautelare



L'evento che si è verificato deve coincidere con il tipo di eventi che la regola cautelare mirava a prevenire



L'evento che si è verificato doveva essere **concretamente evitabile** con la condotta osservante la regola

Grado della colpa

- **Colpa cosciente**
  - L'agente agisce nonostante la previsione dell'evento (art. 61 n.3 c.p.)
- **Colpa incosciente**
  - L'agente agisce non avendo previsto ciò che doveva e poteva prevedere

Dolo eventuale/colpa cosciente

- In entrambi vi è la **previsione** dell'evento dannoso o pericoloso

Tuttavia:

- Nel **dolo eventuale**: vi è indifferenza rispetto alla concreta verificazione dell'evento
- Nella **colpa cosciente**: vi è l'erronea convinzione che l'evento non si verifcherà

La disciplina dell'errore

L'errore sulla legge penale

Art. 5 c.p.

Nessuno può invocare a propria scusa l'ignoranza della legge penale

- **Obbligo generale di conoscenza** del precetto penale
- **Irrilevanza**, ai fini della punibilità, **dell'effettiva ignoranza** della norma incriminatrice

Corte Costituzionale 364/1988

La Corte "*dichiara l'illegittimità costituzionale dell'art. 5 c.p. nella parte in cui non esclude dall'inescusabilità dell'ignoranza della legge penale l'**ignoranza inevitabile***"

Non si può pretendere dall'agente la conoscenza del precetto (per ragioni soggettive o oggettive)

È esclusa la responsabilità penale (per difetto di colpevolezza)

Es.: lo straniero appena giunto su suolo italiano

L'errore sul fatto

Art. 47 c.p.

L'errore sul fatto che costituisce il reato esclude la punibilità dell'agente

L'errore esclude il dolo

L'errore rilevante

- L'errore deve cadere su un elemento **essenziale** da cui dipenda la tipicità del fatto
  - Es.: il soggetto che commetta atti sessuali con un'altra, ignorando che è sua madre, **non** risponde di incesto (errore rilevante)
  - Es. *contra*: chi uccide un uomo, ignorando che sia suo padre, risponde **comunque** di omicidio (errore irrilevante)

L'errore colpevole

Art. 47, c.p.

*Se si tratta di errore determinato da **colpa**, la punibilità non è esclusa, quando il fatto è preveduto dalla legge come delitto colposo*

…Segue

- L'agente cade in errore **per colpa**
  - Per negligenza, imprudenza, imperizia
  - Per inosservanza di leggi, regolamenti, ordini o discipline
- il reato è previsto dal legislatore come **delitto colposo**

Es.: credendo erroneamente di colpire un cadavere, l'agente spara ad un soggetto addormentato. In questo caso risponde per omicidio colposo

L'errore su legge extrapenale

Art. 47, III comma, c.p.

L'errore su una **legge diversa dalla legge penale** esclude la punibilità quando ha cagionato un errore sul fatto che costituisce reato

Il legislatore riserva a questo errore la medesima disciplina dell'errore sul fatto

… Segue

Quando la legge extrapenale spiega il concetto normativo

Si ricade nell'ambito di applicazione dell'art. 5 c.p. con conseguente irrilevanza dell'errore

---

Quando la legge extrapenale serve ad applicare il concetto normativo ai casi concreti

L'errore incide sul fatto e, quindi, esclude il dolo, ex art. 47 c.p.

L'errore sulle scriminanti

Art. 59 c.p.

Se l'agente ritiene per errore che esistano cause di esclusione della pena, queste sono ***sempre valutate a favore di lui****. Tuttavia, se si tratta di errore determinato da colpa, la punibilità non è esclusa, quando il fatto è preveduto dalla legge come delitto colposo*

…Segue

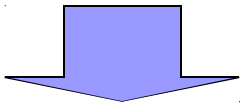
- Stessa disciplina dell'errore sul fatto
- Non vi rientra l'errore sull'esistenza di un diritto o di un dovere scriminante (errore sulla illiceità penale)

Le forme di manifestazione del reato

Il delitto tentato

Il reato consumato

Il reato è consumato quando si verificano tutti i suoi elementi essenziali e tipizzanti



- Nei reati di condotta: quando si compie l'intera azione vietata o si omette di compiere la condotta doverosa
- Nei reati di evento: quando si realizza l'evento

Il delitto tentato

Art. 56 c.p.

*Chi commette **atti idonei**, **diretti in modo non equivoco** a commettere un delitto, risponde di delitto tentato, se l'azione non si compie o l'evento non si verifica*

Le ragioni della rilevanza del tentativo

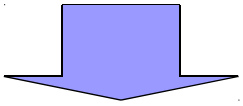
Si intende evitare che si giunga all'effettiva **lesione** del bene giuridico

Si **anticipa** la soglia della rilevanza penale, punendo la mera **messa in pericolo** del bene protetto

I delitti tentati sono, pertanto, **reati di pericolo**

La configurabilità del tentativo

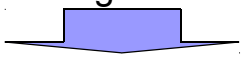
Generalizzazione dell'anticipazione della tutela



- Previsione di una norma di parte generale per la repressione del tentativo (art. 56 c.p.)
- Applicazione della norma di parte generale a tutte le fattispecie di parte speciale
- Tentativo come titolo autonomo di reato

… Segue

In ragione delle sue caratteristiche, il tentativo **non** è configurabile



- Nelle **contravvenzioni** *("delitto tentato"):* la minore gravità priva di giustificazione l'anticipazione della tutela
- Nei **reati di pericolo**: si intende evitare l'anticipazione eccessiva della tutela
- Nei **delitti di attentato**: si tratta di delitti tentati espressamente tipizzati in fattispecie di parte speciale (il tentativo coincide con la consumazione)

L'univocità degli atti

Le azioni già svolte devono rendere riconoscibile ad un osservatore esterno l'intenzione criminosa

Atti esecutivi dell'azione

Sono **esclusi** gli atti preparatori (ossia gli atti che precedono il passaggio all'azione criminosa)

L'idoneità degli atti

- **Adeguatezza causale** degli atti compiuti rispetto alla commissione del reato
- La valutazione deve essere effettuata *ex ante*
  - **Prognosi a base totale**: tutte le circostanze esistenti al momento della commissione, anche se non conoscibili dall'agente
  - Rifiutata in dottrina *(prognosi a base parziale: solo le circostanze conoscibili e non quelle eccezionali ed imprevedibili)*

Il reato impossibile

Art. 49, II comma, c.p.

La punibilità è esclusa quando, per la inidoneità dell'azione o per la inesistenza dell'oggetto, è impossibile l'evento dannoso o pericoloso

- **Inidoneità dell'azione**
  - Es: l'agente spara all'indirizzo di un terzo con una pistola giocattolo
- **Inesistenza dell'oggetto**
  - Es: un borseggiatore inserisce la mano nella borsa di un terzo che si rivela vuota

Desistenza volontaria

Art. 56, III comma, c.p.

Se il colpevole volontariamente desiste dall'azione, soggiace soltanto alla pena per gli atti compiuti, qualora questi costituiscano per sé un reato diverso

Causa di non punibilità a titolo di tentativo

Es: un rapinatore a mano armata entra in una banca ma, di sua spontanea volontà, desiste dal portare a termine la rapina.

Non risponde di tentativo di rapina, ma, laddove l'arma non fosse legittimamente detenuta, solo di porto abusivo di arma

Recesso attivo

Art. 56, IV comma, c.p.

Se il colpevole volontariamente impedisce l'evento, soggiace alla pena stabilita per il delitto tentato, diminuita da un terzo alla metà

- La punibilità **non è esclusa** perché l'agente ha portato a termine la sua condotta criminosa
- Causa di diminuzione della pena

Le forme di manifestazione del reato

Il concorso di persone

Il concorso di persone

Art. 110 c.p.

Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita

I requisiti del concorso

- Commissione di un **fatto costituente reato**
- **Pluralità di persone**
  - Se la fattispecie incriminatrice prevede una pluralità di persone: reati a concorso necessario (es.: rissa)
  - Se la fattispecie incriminatrice non prevede pluralità di persone: reati a concorso eventuale
- **Contributo materiale o morale** dei compartecipi alla commissione del reato

Le condotte rilevanti (concorso materiale)

- L'azione può consistere indifferentemente in un'azione o in un omissione (se esiste posizione di garanzia)
- **Condotte tipiche:** ciascuno dei concorrenti contribuisce alla consumazione del reato compiendo un'azione tipizzata nella fattispecie incriminatrice
  - Es.: due soggetti commettono una rapina a mano armata: uno punta la pistola sulla vittima e l'altro si fa consegnare la borsa
- **Condotte atipiche** (se afferenti ad un fatto tipico): uno o più concorrenti partecipano alla commissione del reato tenendo condotte non espressamente tipizzate dal legislatore
  - Es.: nel caso di rapina ad una banca, il palo che attende fuori dall'edificio partecipa a titolo di concorso nella rapina

Il contributo causale della condotta dei compartecipi

Il compartecipe deve fornire con la propria azione un **contributo causale** alla complessiva organizzazione dell'impresa delittuosa

Verifica del nesso causale tra la condotta del compartecipe e la realizzazione del fatto criminoso

Teoria della *conditio sine qua non*

Teoria della causalità agevolatrice

Il concorso morale

Risponde di concorso morale chi

- Fa nascere in altri il proposito di commettere reato (determinazione)
- Rafforza un proposito già esistente (istigazione)

Requisiti

- Deve rivolgersi a destinatari ben definiti
- Deve avere ad oggetto un fatto concretamente determinato

Le forme di manifestazione del reato

Il concorso di reati

Concorso apparente di norme

- **Principio di specialità:** quando due norme sono in rapporto di specialità l'una con l'altra, si applica solo la norma speciale
  - Es: il reato di furto, se commesso con violenza o minaccia, integra il reato di rapina
- **Criterio di sussidiarietà:** il legislatore stesso riserva un'applicazione residuale alla norma
  - Es: *"salvo che il fatto non costituisca più grave reato"* (istigazione dei militari a disobbedire alle leggi)
- **Criterio dell'assorbimento:** gli antefatti e i postfatti non costituiscono reati se seguiti o preceduti da altro reato più grave
  - Es: contraffazione di carta filigranata è assorbito dal reato di fabbricazione di falsa moneta.

Concorso materiale

Con più azioni od omissioni il reo commette più reati

Si applica il c.d. **cumulo materiale**

La pena complessiva è calcolata sommando le pene applicate a ciascuno dei reati commessi (nei limiti del quintuplo della pena più grave)

Concorso formale

Art. 81 c.p.

Il concorso formale consiste nella condotta di chi *"con una sola azione od omissione viola diverse disposizioni di legge o commette più violazioni della medesima disposizione di legge"*

Si applica il c.d. **cumulo giuridico**

pena prevista per il reato più grave aumentata sino al triplo

Continuazione

Art. 81, comma II, c.p.

Incorre in continuazione chi *"con più azioni od omissioni, in applicazione del medesimo disegno criminoso, commette anche in tempi diversi più violazioni della medesima disposizione di legge"*

Anche in questo caso si applica il

cumulo giuridico

Le forme di manifestazione del reato

Il reato circostanziato

I tipi di circostanze

- Circostanze attenuanti o aggravanti
  - A seconda degli effetti che producono sulla pena
- Circostanze comuni o speciali
  - A seconda che siano previste per la generalità dei reati o solo per alcuni
- Circostanze tipiche o generiche
  - A seconda che siano espressamente tipizzate o lasciate alla discrezionalità del giudice
- Circostanze a effetto comune o a effetto speciale
  - A seconda dell'entita della modifica che apportano alla pena base

I criteri di imputazione delle circostanze

Circostanze aggravanti
(imputazione soggettiva)

- Devono essere conosciute dall'agente o ignorate per colpa
- Principio di colpevolezza

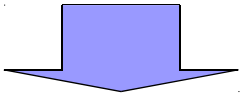
Circostanze attenuanti
(imputazione oggettiva)

- Si applicano anche se non conosciute dall'agente
- Non si applicano se erroneamente ritenute esistenti (art. 59 c.p.)

La commisurazione della pena

Il sistema sanzionatorio

Il “Codice Rocco” introduce il sistema del c.d. “doppio binario”:



Pene

Misure di sicurezza

Le specie di pene: richiamo

- Per i **delitti**:
  - Ergastolo
  - Reclusione
  - Multa
- Per le **contravvenzioni**:
  - Arresto
  - Ammenda

All'interno di ogni fattispecie di parte speciale è prevista una comminatoria edittale, con la previsione di un minimo ed un massimo di pena

La commisurazione della pena

Art. 132 c.p.

*Nei limiti fissati dalla legge, il giudice applica la pena **discrezionalmente**; esso deve indicare i **motivi** che giustificano l'uso di tale potere discrezionale*

Sussiste in capo al giudice l'**obbligo di motivazione**

I criteri per la commisurazione della pena (art. 133 c.p.)

Il Giudice è vincolato, nell'esercizio del potere discrezionale, alla valutazione

- Della **gravità del reato**
  - Natura, specie, mezzi, oggetto, tempo, luogo e ogni altra modalità dell'azione
  - Intensità del dolo o grado della colpa
  - Gravità del danno o del pericolo cagionato
- Dalla **capacità a delinquere del reo**
  - Motivi a delinquere e carattere del reo
  - Precedenti penali e giudiziari e condotta di vita antecedente al reato
  - Condotta contemporanea o susseguente al reato
  - Condizioni di vita individuale, familiare e sociale

La commisurazione della pena pecuniaria

Nell'applicazione della pena pecuniaria il giudice deve tenere conto

- Della gravità del reato
- Della capacità a delinquere del reo
- Delle **condizioni economiche del reo** (art. 133 *bis* c.p.)

- Se anche il minimo risulta troppo gravoso, il giudice può ridurre sino ad un terzo
- Se il massimo risulta inefficace, il giudice può aumentare sino al triplo

La pena nel reato circostanziato
Il giudizio di bilanciamento

- Se esistono solo aggravanti:
  - Il giudice applica gli aumenti di pena, nella misura prescritta, uno dopo l'altro
- Se esistono solo attenuanti:
  - Il giudice applica le diminuzioni di pena una dopo l'altra
- Se concorrono circostanze eterogenee:
  - Se il giudice ritiene prevalenti le aggravanti;
    - Applica le sole aggravanti, senza tenere conto delle attenuanti
  - Se il giudice ritiene prevalenti le attenuanti:
    - Applica le sole attenuanti, senza tenere conto delle aggravanti
  - Se il giudice ritiene equivalenti aggravanti ed attenuanti:
    - Applica la pena base, come se il reato non fosse circostanziato

Le misure di sicurezza
I requisiti per l'applicazione

- Commissione di un **reato** o di un **quasi-reato** (non è necessaria la condanna)
  - Delitto o contravvenzione
  - Reato impossibile
  - Accordo per commettere un delitto
- **Pericolosità sociale:** giudizio prognostico sulla probabile commissione di altri delitti

Le misure si sicurezza

Detentive

- Ospedale psichiatrico giudiziario (non imputabili)
- Casa di cura e custodia (semi imputabili)
- Casa di lavoro o colonia agricola (imputabili)

Non detentive

- Libertà vigilata

Patrimoniali

- Confisca
- Cauzione di buona condotta

La nascita di nuove esigenze di tutela

La nascita di nuove esigenze di tutela

- Nel corso degli anni ’70, la diffusione dei primi sistemi informatici ha dato avvio ad una serie di **fenomeni criminosi connessi con il mezzo informatico**

- Il sistema penale allora vigente non consentiva la punizione di tali fenomeni

Una definizione di reato informatico

- Computer crimes o *computer-related crimes*?
- **Conoscenza della tecnologia informatica**
  - non essenziali alla realizzazione del reato e (in ogni caso) irrilevanti se non utilizzato un sistema informatico
- **Utilizzo di un qualsiasi tipo di elaboratore**
  - In tal modo, si riconducono alla categoria tutti i reati in cui il collegamento con l'elaboratore sia anche solo casuale
- **Il computer è oggetto o strumento dell'azione**
  - Vengono ricondotti alla categoria sia forme di aggressione alla componente materiale che alla componente logica
  - Possibilità di una definizione mirata alla sola componente immateriale del sistema informatico (escluso, tuttavia, il "furto di tempo")

La classificazione delle condotte

- **Manipolazioni di dati** *(Computermanipulationem)*
  - Impiego fraudolento dell'elaboratore per procurarsi un ingiusto vantaggio economico
- **Sabotaggio informatico** *(Computersabotage)*
  - Danneggiamento di dati e programmi
- **Spionaggio informatico** *(Computerspionage)*
  - Indebita acquisizione di dati e programmi immagazzinati in un elaboratore
- **"Furto di tempo"** *(Zeitdiebstahl)*
  - Uso non autorizzato del tempo di elaborazione di un sistema informatico altrui

Le spinte internazionali

Metà degli anni '80

- Studio sulla criminalità organizzata OCSE
- Rapporto del Comitato europeo per i problemi criminali

13 settembre 1989

- Raccomandazione n. R (89) 9, *"sur la criminalité en relation avec l'ordinateur"* – Comitato dei Ministri del Consiglio d'Europa

Lista minima

Condotte di abuso dell'elaboratore senz'altro ritenute meritevoli di sanzione penale

- Frode informatica
- Falso in documenti informatici
- Danneggiamento di dati e programmi
- Sabotaggio informatico
- Accesso non autorizzato ad un sistema informatico
- Intercettazione non autorizzata di comunicazioni informatiche
- Riproduzione non autorizzata di un programma protetto
- Riproduzione non autorizzata della topografia di un prodotto a semiconduttori

Lista facoltativa

Condotte la cui repressione penale è rimessa alla valutazione della legislazione nazionale

- Alterazione di dati o di programmi
- Spionaggio informatico
- Utilizzazione non autorizzata di un elaboratore
- Utilizzazione non autorizzata di un programma informatico

Le indicazioni dell'AIDP

Rio de Janeiro, settembre 1994

- Commercio di codici d'accesso ottenuti illecitamente o di altre informazioni sulla possibilità di conseguire un accesso non autorizzato a sistemi informatici
- Diffusione di programmi virus o programmi similari
- Invito a considerare l'opportunità di sanzionare anche condotte colpose

Convenzione sul Cybercrime

Budapest, 2001

- Reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici
  - Accesso abusivo
  - Intercettazione di comunicazioni informatiche
  - Danneggiamento di dati
  - Sabotaggio di sistemi informatici
  - Commercio di strumenti finalizzati alla commissione di uno dei reati precedenti
  - Commercio di password
- Reati commessi con il mezzo informatico
  - Falso informatico
  - Frode informatica

Le condotte escluse

Gli illeciti non riconducibili ai reati informatici

- le violazioni della *privacy* attraverso la raccolta e la gestione di **dati personali**
- i reati (diversi da quelli informatici) commessi attraverso **Internet**

La legislazione italiana

- L. 5 luglio 1991, n. 197
  - Abuso di carte di pagamento
- L. 23 dicembre 1993, n. 547
  - Introduzione nel codice penale dei reati informatici
- L. 18 marzo 2008, n. 48
  - Ratifica della Convenzione di Budapest del 2001 (e riforma delle fattispecie di reato)

La scelta classificatoria

- Nuove modalità di aggressione a beni giuridici già oggetto di tutela penale
  - Delitti contro la persona
  - Delitti contro il patrimonio
  - Delitti contro la fede pubblica
- Collocazione in prossimità delle fattispecie di reato già esistenti, che sarebbero integrate laddove il reato non fosse compiuto con il mezzo informatico

Delitti contro il patrimonio

- **Delitti di frode**
  - Frode informatica (art. 640 *ter* c.p.)
  - Abuso di carte di pagamento elettroniche (art. 12, l. 197/1991)
- **Delitti di aggressione all'integrità di dati e programmi**
  - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies c.p.*)
  - Delitti di danneggiamento informatico (artt. 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies*)

Delitti contro la persona

- **Delitti di aggressione alla riservatezza dei dati**
  - Accesso abusivo (art. 615 *ter* c.p.)
  - Diffusione di codici di accesso (art. 615 *quater* c.p.)
  - Rivelazione del contenuto di documenti informatici segreti (art. 621 c.p.)
- **Aggressioni alla riservatezza delle comunicazioni informatiche**
  - Violazione di corrispondenza informatica (art. 616 c.p.)
  - Intercettazione di comunicazioni informatiche (artt. 617 *quater* e *quinquies* c.p.)

Delitti contro la fede pubblica

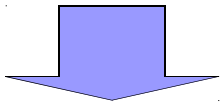
- Falsificazione del contenuto di comunicazioni informatiche (art. 617 *sexies* c.p.)
- Falsità in documenti informatici (art. 491 *bis* c.p.)
- Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri

La frode informatica

Le condotte di manipolazione dei dati

Le categorie

- **Manipolazioni di dati**
  - input, output
- **Manipolazioni di programma**
- **Manipolazioni di hardware**



Il risultato finale sarà sempre un **output falso**

Manipolazione di input

Esempio

Il dipendente di una società introduce dati falsi attraverso il suo terminale, per far risultare il nominativo di sua sorella tra quelli dei dipendenti della società, per i quali ogni mese il computer provvede al calcolo dello stipendio e alla emissione della relativa busta paga

Introduzione di dati falsi

…Segue

Esempio

Il funzionario di una banca modifica i dati relativi ai bonifici effettuati a favore dei clienti, aumentandone l'importo; provvede poi a stornare la somma in eccesso sul proprio conto corrente

Modifica di dati veri

… Segue

Esempio

Una persona preleva del denaro da un distributore automatico di banconote, utilizzando abusivamente la carta Bancomat intestata ad un'altra persona e il relativo numero di identificazione personale (PIN)

Introduzione di dati 'altrui'

Manipolazione di output

Esempio

I gestori di un sistema di scommesse sulle corse dei cani alteravano i dati finali sul numero dei giocatori vincenti, calcolato dall'elaboratore al termine di tre gare consecutive, in modo da ridurre il valore della singola vincita, in conseguenza dell'inserimento di nominativi di persone fittizie

Manipolazione di programma

Esempio

Un programmatore, incaricato da una banca della redazione di un programma per il calcolo degli interessi passivi da pagare ai clienti, inserisce un'istruzione che arrotonda per difetto, anziché per eccesso, gli interessi dei correntisti e fa confluire la differenza sul conto corrente del programmatore

Creazione di un programma 'contrario al sistema'

Manipolazione di consolle

Esempio

Un ex-dipendente di un commerciante si reca da quest'ultimo per effettuare un acquisto; al momento di pagare la merce, approfittando della distrazione del commesso, preme un particolare tasto del registratore di cassa che determina l'applicazione di uno sconto del 70% sulla spesa effettuata; sconto al quale egli non aveva alcun diritto, non essendo più dipendente di quel esercizio commerciale

Manipolazione di consolle

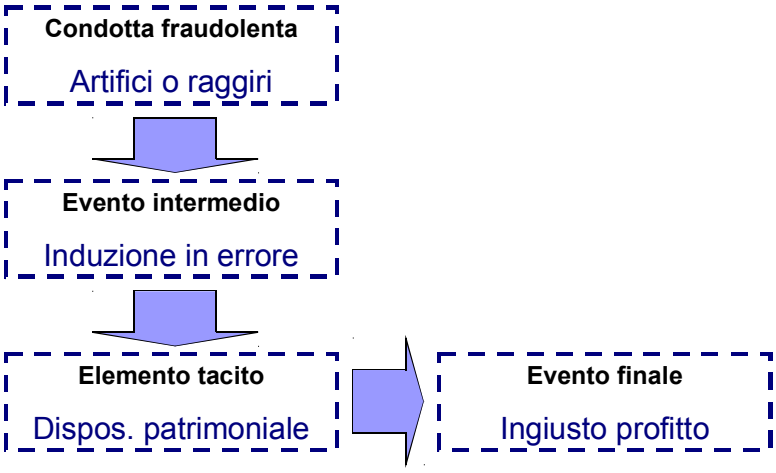
La fattispecie base di truffa *ex* art. 640 c.p. e la rilevanza delle frodi informatiche prima della legge 547/1993

La fattispecie di truffa

Art. 640 c.p.

*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 6 mesi a 3 anni e con la multa da euro 51 a euro 1.032*

Gli elementi essenziali del reato



Estensione della truffa alle condotte di manipolazione di dati?

Elemento essenziale della truffa *ex* art. 640 c.p. è l'**induzione in errore di un essere umano**

- Tale elemento non è sempre presente nelle frodi informatiche
- Occorrerebbe verificare il controllo del risultato dell'elaborazione da parte di un essere umano

La posizione della giurisprudenza

T. Roma, 14 dicembre 1985

Il dipendente bancario che, inserendo dati falsi nell'elaboratore, rappresenta falsamente che alcuni versamenti sono avvenuti in contanti anziché in assegni, onde occultare il maggior rischio assunto con la negoziazione di assegni prima di averne avuto confermata la copertura e procurare il maggior lucro ai correntisti attraverso il riconoscimento della valuta liquida, pone in essere artifici idonei a trarre in inganno gli organi di controllo della banca, e commette il reato di truffa aggravata

…Segue

T. Roma, 20 giugno 1985

Configura il reato di **truffa** l'induzione in errore di funzionari dell'INPS, preposti al controllo del versamento ed all'esazione dei contributi previdenziali, attraverso l'immissione nell'elaboratore elettronico di dati non veritieri sui pagamenti effettuati

… Segue

Cass. 7 dicembre 1989

Configura il reato di furto con mezzi fraudolenti il prelievo di somme da sportelli automatici del sistema Bancomat, mediante carta contraffatta

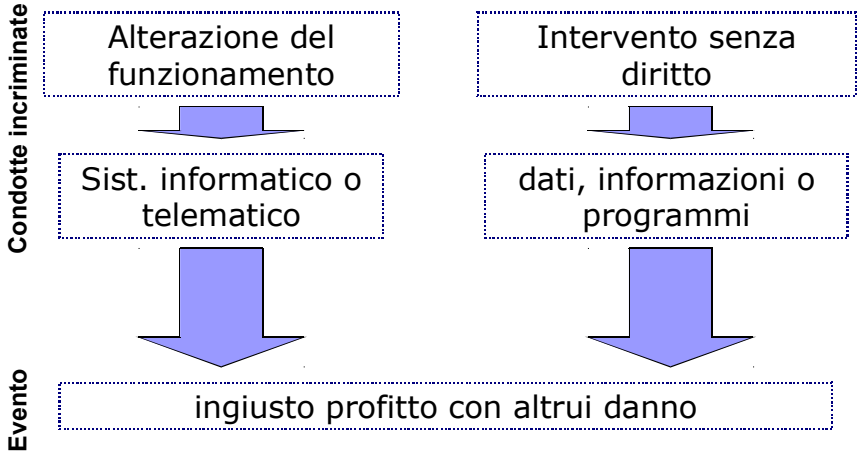
La nuova fattispecie di frode informatica

La frode informatica

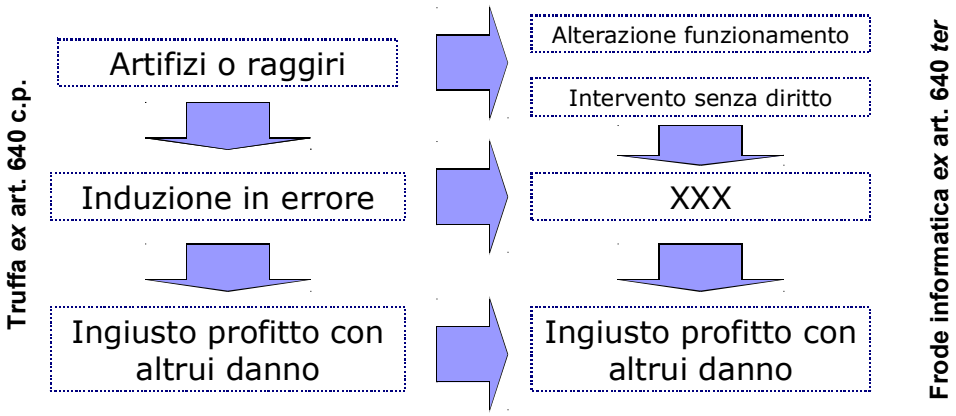
Art. 640 *ter* c.p.

*Chiunque, **alterando** in qualsiasi modo **il funzionamento di un sistema informatico** o telematico o **intervenendo senza diritto** con qualsiasi modalità **su dati, informazioni o programmi** contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un **ingiusto profitto** con altrui danno, è punito con la reclusione da 6 mesi a 3 anni e con la multa da euro 51 a euro 1.032*

Gli elementi essenziali della frode informatica



Frode informatica e truffa



Il sistema informatico o telematico

Sistema informatico

- qualunque sistema di per il trattamento automatizzato dei dati
- anche una carta a microprocessore e gli apparecchi che erogano beni o servizi

Sistema telematico

- qualunque sistema informatico connesso ad una rete di trasmissione dati

Dati, informazioni e programmi

- **Dati**
  - informazioni espresse in forma comprensibile per l'elaboratore
- **Informazioni**
  - informazioni espresse in linguaggio alfanumerico, comprensibile all'uomo
- **Programmi**
  - insieme di istruzioni per l'elaboratore, espresse in forma di dati

Le condotte punibili

- **Alterazione del funzionamento del sistema informatico**
  - manipolazione di hardware
  - manipolazione di programma
- **Intervento senza diritto su dati, informazioni e programmi**
  - manipolazione di input
  - manipolazione di programma
  - manipolazione di output

L'introduzione di dati nuovi

- L'intervento sui dati (previsto dalla norma) prevede una loro **modificazione**
- L'inserimento di dati nuovi comporta **intervento senza diritto sui dati già esistenti in memoria**, ai quali i primi vengono ad aggiungersi

L’introduzione di dati altrui

Si ha un intervento senza diritto sui **dati relativi al titolare**, che subiscono una modifica in conseguenza della operazione effettuata ai suoi danni

Es.: PIN per servizi di home banking

La circostanza aggravante

La pena è della reclusione da 1 a 5 anni e della multa da euro 309 a euro 1.549 […] se il fatto è commesso con abuso della qualità di operatore del sistema

Operatore di sistema

Tecnico che ha il controllo di tutte le fasi del processo di elaborazione dei dati *(amministratore di sistema)*

Casistica giurisprudenziale
Differenze tra truffa e frode informatica

Cass. Pen., sez. II, 11.11.2009, n. 44720

Il reato di frode informatica si differenzia dal reato di truffa perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema

Casistica giurisprudenziale
Bene giuridico tutelato

Cass. Pen., Sez. V, 24.11.2003, n. 4576

La norma di cui all'art. 640 ter c.p. è posta a tutela sia della riservatezza e della regolarità dei sistemi informatici che del patrimonio altrui […]

Casistica giurisprudenziale
Le condotte rilevanti

Tribunale Torino, 4.12.1997

La mera duplicazione delle procedure informatiche facenti parte del patrimonio aziendale non configura il reato di frode in quanto non integra un'iniziativa volta a cagionare dolosamente al titolare dell'impresa un danno al funzionamento o ai risultati del sistema

Casistica giurisprudenziale
Le condotte rilevanti

Il caso Telecom

L'agente, utilizzando il sistema telefonico fisso installato in una filiale della società italiana per l'esercizio telefonico, con la veloce e ininterrotta digitazione di numeri telefonici, in parte corrispondenti a utenze estere, riusciva ad ottenere collegamenti internazionali, eludendo il blocco predisposto per tali chiamate per le quali il sistema non era abilitato, così esponendo debitoriamente la società italiana per l'esercizio telefonico nei confronti dei corrispondenti organismi esteri autorizzati all'esercizio telefonico

Casistica giurisprudenziale

Le condotte rilevanti

Tribunale di Lecce, 12.03.1999

Integra il delitto di frode informatica la condotta di chi mediante la digitazione su apparecchi telefonici collegati a linee interne di una filiale Telecom, di una particolare sequenza di cifre, effettui una serie di chiamate internazionali in danno della Telecom, tenuta a versare agli enti gestori della telefonia bei paesi di destinazione dell'importo corrispondente al suddetto traffico telefonico.

Casistica giurisprudenziale

Le condotte rilevanti

Tribunale di La Spezia, 23.09.2004

Sussistono gli estremi della frode informatica nel comportamento di chi attiva un programma dialer nell'altrui sistema informatico, provocando l'interruzione del programma di connessione telefonica instaurando un successivo collegamento con linee a pagamento, cui consegue un aumento non voluto dei costi della connessione telefonica

Casistica giurisprudenziale

Le condotte rilevanti

Tribunale di Genova, 27.09.1999

Sussistono gli estremi della frode informatica nel comportamento di chi utilizza un telefono cellulare clonato su numero intestato a diverso utente, così alterando il funzionamento del sistema telematico connesso a quello di telefonia mobile, con danno per l'intestatario dell'utenza clonata e per la Telecom

L’abuso di carte di pagamento

Aggiungere un testo con un clic

L’abuso di carte di pagamento

Art. 12, comma I, legge 197/1991

*Chiunque, al fine di trarne profitto per sé o per altri, indebitamente **utilizza**, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all’acquisto di beni o alla prestazione di servizi, è punito con la reclusione da 1 a 5 anni e con la multa da 309,87 euro a 1549,37 euro”.*

Falsificazione e alterazione di carte di pagamento
Possesso, cessione e acquisizione di carte di pagamento contraffatte

Art. 12, comma II, legge 197/1991

Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, **falsifica** o **altera** carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero **possiede**, **cede** o **acquisisce** tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi".

Gli abusi rilevanti

- Abuso da parte di terzi
  - carta altrui: rilevante ai sensi del comma I dell'art. 12, l. 197/91
  - carta falsa: rilevante ai sensi del comma II dell'art. 12, l. 197/91
- Abuso da parte del titolare: integrato, ai sensi del I comma, qualora difetti la legittimazione all'utilizzo della carta
  - carta revocata (Cass. 12.11.1996 e 11.11.2003)
  - carta scaduta (Cass. 28.11.1997)

Le tipologie di carte di pagamento

- Carte di credito
  - Bilaterale
  - trilaterale
- Carte di debito
  - come carte di prelievo
  - come carte di pagamento
  - carte prepagate (se nominative)
- Carte-assegni
  - sì Cass. 27 gennaio 1992
  - no Cass. 13 aprile 2000

Le condotte incriminate

- **Indebito utilizzo (comma I)**
  - di carta altrui o di carta scaduta e/o revocata
- **Falsificazione o alterazione (comma II)**
  - ipotesi speciale di falsità in scrittura privata
- **Possesso di carta di provenienza illecita o falsa (comma II)**
  - anticipazione della tutela
- **Cessione o acquisizione di carte di provenienza illecita (comma II)**
  - ipotesi speciale di ricettazione

T. Torino, 11 maggio 1994

L'indebita utilizzazione di carte di credito falsificate … deve considerarsi integrata anche dal semplice tentativo di far passare la carta falsa nel POS di un negozio, poiché se l'autorizzazione negativa proveniente dall'emittente non permette il completamento dell'operazione di spesa, comunque la carta artefatta mediante l'illecita ricostruzione su di essa di banda magnetica di altra carta di credito risulta essere già stata usata ed aver messo in funzione tutta la rete di trasmissione di dati tra singolo POS ed emittente".

Cass. 16 dicembre 1997

Integra il reato consumato, e non semplicemente tentato, di indebita utilizzazione di carte di credito e di altri strumenti di pagamento la consegna di tessera "Viacard" all'incaricato dell'esazione del pedaggio al casello autostradale da parte di persona non titolare di essa, in quanto tale volontaria consegna costituisce già pieno utilizzo della carta medesima, restando irrilevante, ai fini della consumazione, che l'utilizzazione non raggiunga effettivamente lo scopo di vedere addebitato alla carta l'importo corrispondente al pedaggio a seguito della riconosciuta illiceità dell'operazione, accertata in tempo reale dalla macchina esattrice collegata alla rete informatica propria del circuito di pagamento".

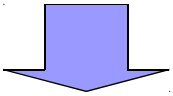
Rilevanza penale dell'abuso

Al fine di definire l'**indebito utilizzo**

- utilizzare significa usare utilmente
- non è, dunque, sufficiente un qualsiasi impiego della carta
- occorre piuttosto che l'uso abbia arrecato l'utilità che è propria della carta (accettazione come mezzo di pagamento o di prelievo)

Cass. 24 aprile 1996

Commette il delitto di tentativo di indebita utilizzazione di una carta di pagamento colui che introduca una carta "Bancomat" di illecita provenienza in uno sportello automatico e, non disponendo del codice di accesso, esegua una serie di combinazioni numeriche al fine di conseguire il denaro, senza riuscirvi".



Reato impossibile (art. 49 c.p.)

La posizione della giurisprudenza

- la giurisprudenza riconduce alla fattispecie di indebito utilizzo tutti gli abusi di carte di pagamento altrui o di carte false;
- qualsiasi uso della carta di pagamento viene punito, anche se concretamente inidoneo a ledere il patrimonio altrui

L'accesso abusivo a sistemi informatici protetti

Il dato criminologico

- Spionaggio informatico: accesso non autorizzato ed eventuale divulgazione di segreti
  - Industriali
  - Commerciali
  - Militari
- Aggressioni degli *hacker*: accessi non autorizzati a sistemi informatici o telematici protetti

…e le conseguenti esigenze di tutela

- Particolare vulnerabilità delle informazioni rappresentate da dati
- Insufficienza delle difese di tipo tecnico
- Inadeguatezza delle fattispecie penali tradizionali
  - reati contro l'inviolabilità dei segreti
  - reati contro il patrimonio

I reati contro l'inviolabilità dei segreti

- **Rivelazione del contenuto di documenti segreti** (art. 621 c.p.)
  - Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto
- **Rivelazione di segreto professionale** (art. 622 c.p.)
  - Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto.
- **Rivelazione di segreti scientifici o industriali** (art. 623 c.p.)
  - Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto.

Le ragioni dell'inadeguatezza

- Il riferimento agli *"atti o documenti"* non consente l'estensione ai *"dati o programmi"*
- il riferimento alla ragione d'ufficio o di servizio restringe l'area del penalmente rilevante, escludendo le condotte di coloro che accedano ai *segreti* indipendentemente dalla loro occupazione
- Il requisito della divulgazione è spesso incompatibile con le condotte degli *hacker*

… una precisazione

L'inadeguatezza delle fattispecie di *rivelazione di segreti* non ne esclude sempre l'applicabilità ai reati informatici

Cass. Pen., sez. IV, 21.12.2010, n. 44840

Commette il reato di cui all'art. 622 c.p., per il quale l'azione costitutiva consiste nel rivelare il segreto o nell'impiegarlo a proprio o altrui profitto, l'impiegato di una società, che trasmetta – nel caso di una gara di appalto – notizie segrete riguardanti la sua azienda a vantaggio della società poi rimasta aggiudicataria dei lavori.

Il furto di dati

Art. 624 c.p.

*"Chiunque si impossessa della **cosa mobile** altrui, **sottraendola** a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da 6 mesi a 3 anni e con la multa da euro 154 a euro 516"*

i dati non sono 'cose'

la loro duplicazione non comporta spossessamento del detentore

La posizione della giurisprudenza

Cass. 13 novembre 2003

*La copiatura dei files da CD o da HD in altro non consiste se non in una 'duplicazione' di tali files (analoga al risultato di un procedimento fotografico), tanto che i files in possesso del detentore del CD o del computer sul quale sia installato l'hard-disk contenente i files **rimangono memorizzati sul medesimo supporto** sul quale si trovavano, mentre di essi il soggetto entra in possesso di una copia. Ne consegue la non configurabilità del reato di furto*

Il nuovo reato di accesso abusivo

Aggiungere un testo con un clic

La soluzione italiana

Due nuovi reati, inseriti tra i delitti contro **l'inviolabilità del domicilio**

Accesso abusivo ad un sistema informatico

(art. 615 *ter* c.p.)

Diffusione di codici di accesso a sistemi informatici

(art. 615 *quarter* c.p.)

Accesso abusivo ad un sistema informatico

Art. 615-ter c.p.

"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 3 anni".

Raffronto con la violazione di domicilio

Art. 614 c.p.

*Chiunque **si introduce** nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero **vi s'introduce** clandestinamente o con inganno, è punito con la reclusione fino a tre anni.*

*Alla stessa pena soggiace chi **si trattiene** nei detti luoghi contro l'espressa volontà di chi ha diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno.*

Il bene giuridico tutelato

Possibili beni giuridici tutelati dalla norma:

- **Domicilio informatico**
- **Integrità** dei dati e dei programmi
- **Riservatezza** dei dati e dei programmi

L'art. 615 *ter* c.p. tutela il domicilio informatico?

- **A sostegno:**
  - collocazione sistematica
  - lavori preparatori (art. 14 Cost.)
- **Contro:**
  - non è un luogo di proiezione spaziale della persona
  - la disposizione tutela anche (e soprattutto) computer del settore industriale
  - la norma si applica solo sistemi protetti

L'art. 615 *ter* c.p. tutela l'integrità dei dati?

- **A sostegno**
  - È prevista un'aggravante per danneggiamento
- **Contro**
  - Dato criminologico (il problema non è il danneggiamento)
  - Necessità di misure di sicurezza

L'art. 615 *ter* c.p. tutela il la riservatezza dei dati?

- si concilia con ogni tipo di sistema informatico (sia esso pubblico o privato)
- È coerente con la necessità di protezione (chi non protegge il sistema da ingressi non autorizzati non ha interesse alla riservatezza dei dati in esso contenuti)
- È coerente con l'aggravante di cui al comma III dell'art. 615 *ter* c.p. (prevista quando "*i fatti 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***").

Bene giuridico tutelato e natura del reato

Bene giuridico	Natura del reato
Domicilio informatico	Reato di danno
Integrità dei dati	Reato di pericolo
Riservatezza dei dati	Reato di pericolo

Sistemi informatici oggetto di tutela

Se la norma tutela il domicilio informatico o l'integrità dei sistemi

Tutti i sistemi informatici

Se la norma tutela la riservatezza dei dati

Solo i sistemi funzionali alla raccolta di dati

(con esclusione dei sistemi che erogano solo beni o servizi)

Misure di sicurezza

- Misure di tipo logico (es: password)
- Misure di tipo fisico (es: chiavi di accensione)
  - escluse le misure di protezione del locale in cui si trova il sistema
- Requisiti:
  - Occorre che siano astrattamente idonee a prevenire il tipo di accesso effettivamente realizzato
  - Non è necessario che siano insuperabili (potendo, ad esempio, consistere in password di facile individuazione)

Le condotte punite

- **Introduzione abusiva**
  - accesso alla memoria del sistema
  - non occorre l'acquisizione o la conoscenza dei dati
  - può avvenire da lontano o 'da vicino'
- **Permanenza non autorizzata**
  - presuppone un accesso casuale o autorizzato
  - permanenza all'interno del sistema con la consapevolezza di essere in un sistema protetto e di non avere l'autorizzazione per farlo

Le circostanze aggravanti

Art. 615 *ter* c.p.

"La pena è della reclusione da 1 a 5 anni:
se il fatto è commesso … con abuso della qualità di operatore del sistema"

1. Operatore di sistema: tecnico normalmente non autorizzato a conoscere il contenuto dei dati
2. normalmente l'operatore di sistema effettuerà una **permanenza non autorizzata**

…segue

Art. 615 *ter* c.p.

"La pena è della reclusione da 1 a 5 anni:
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".

L'aggravante opera solo per gli eventi dannosi non voluti. In caso contrario, si ha concorso con il danneggiamento informatico

Il reato di diffusione di codici d'accesso

Detenzione e diffusione abusiva di codici di accesso

Art. 615 *quater* c.p.

*Chiunque, al fine di procurare a sè 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 ad 1 anno e con la multa sino a euro 5.164*

La natura del delitto di diffusione di codici d'accesso

- Punisce le condotte propedeutiche alla realizzazione di un accesso abusivo
- Reato di pericolo necessariamente indiretto
  - pericolo che al reato consegua la commissione di un altro reato di pericolo
  1. un'ulteriore diffusione abusiva
  2. un accesso abusivo

La natura del reato in relazione al bene giuridico tutelato dall'art. 615 *ter* c.p.

Bene giuridico	Natura del 615 ter	Natura del 615 quater
Domicilio informatico	Reato di danno	Reato di pericolo
Integrità dei dati	Reato di pericolo	R. di pericolo indiretto
Riservatezza dei dati	Reato di pericolo	R. di pericolo indiretto

Problema

La legittimità dei reati di pericolo indiretto deve essere valutata in base al **principio di proporzione**

occorre un **ragionevole rapporto** tra **gravità dell'offesa** e **rango** del bene protetto

Nel reato di cui all'art. 615 *quarter* c.p.: **non** c'è proporzione: il fatto punito è molto lontano dalla lesione e coinvolge un bene non di fondamentale importanza per la collettività

Le condotte punite

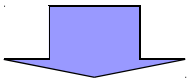
- **Diffusione**
  - ad un numero indeterminato di persone
- **Comunicazione**
  - ad un numero determinato di persone
- **Consegna**
  - di cose materiali (es. budge, chiave)

La detenzione di codici d'accesso

- La detenzione di codici d'accesso non è espressamente prevista quale condotta rilevante ai fini dell'integrazione del reato di cui all'art. 615 *quater* c.p.
- La detenzione, tuttavia, costituisce "indizio" rilevante ai fini della prova di una condotta volta a *procurarsi* codici d'accesso

Sistemi tutelati

Stessa soluzione adottata per il reato di accesso abusivo



1. qualunque sistema (se oggetto di tutela è il domicilio informatico o l'integrità dei dati)

1. solo sistemi funzionali alla raccolta di dati (se oggetto di tutela è la riservatezza dei dati)

Diffusione di programmi virus

La diffusione di programmi virus

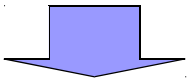
Art. 615 *quinquies* c.p.

*"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"* (*)

(*)Testo precedente alla riforma introdotta con L. 8 marzo 2008, n. 48 *(ratifica della Convenzione di Budapest sul Cibercrime)*

Il bene giuridico tutelato

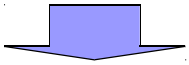
- Nonostante la collocazione sistematica (inviolabilità del domicilio), la norma è finalizzata a proteggere **l'integrità dei dati e dei programmi**



- Punisce, quindi, le condotte prodromiche alla realizzazione di un **danneggiamento informatico**

La natura del reato di cui all'art. 615 *quinquies* c.p.

Reato di **pericolo eventualmente indiretto**



- La condotta può sfociare:
  - Nell'istallazione di un programma virus all'interno di un sistema informatico: danneggiamento informatico (danno)
  - Nell'ulteriore diffusione del programma virus (pericolo)

Il problema di legittimità costituzionale

- La legittimità dei reati di pericolo indiretto va valutata in base al principio di proporzione:
  - ragionevole rapporto tra la gravità dell'offesa che si reprime ed il rango del bene protetto

- Nel caso dell'art. 615 *quinquies* c.p., si registra una potenziale ed incontrollata diffusione del virus

- l'anticipazione della tutela appare giustificabile per l'importanza che l'**integrità ed il buon funzionamento dei sistemi** rivestono per la società e per la gravità del danno che i programmi virus possono provocare

Il nuovo delitto di diffusione di programmi virus

L. 18 marzo 2008, n. 48

Art. 615 *quinquies* c.p.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o ad interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa fino ad € 10.329.

Programmi virus?

- **Strumentazione *hardware***
  - Apparecchiature e dispositivi
- ***Software*** (assente definizione di programmi rilevanti)
  - *Qualsiasi programma che possegga una potenzialità offensiva, anche minima*
    - non si richiede una capacità riproduttiva (bombe logiche)
    - esclusi i programmi che modificano il funzionamento senza arrecare pregiudizio alla funzionalità
- Sono sempre esclusi il programma ancora nella forma del codice sorgente e le informazioni su come creare programmi dannosi

La norma precedentemente in vigore limitava l'ambito di operatività ai soli programmi, senza prendere in considerazione *"apparecchiature e dipositivi"*

Le condotte punite

- **Procurarsi**: Entrare, in qualsiasi modo, in possesso
- **Produrre**: Creare un nuovo strumento offensivo
- **Riprodurre**: Copiare un modello preesistente
- **Importare**: Introdurre all'interno del territorio nazionale
- **Diffondere**: Ad un numero indeterminato di soggetti
- **Comunicare**: Ad un numero determinato di soggetti
- **Consegnare**: mediante cessione anche del supporto materiale

La norma precedentemente in vigore contemplava, quali condotte rilevanti, solo la **diffusione**, la **comunicazione**, la **consegna**

La rilevanza del dolo specifico

allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione totale o parziale, o l'alterazione del suo funzionamento

- l'agente deve prefigurarsi un futuro reato di danneggiamento di
  - *Un sistema informatico o telematico*
  - *Dati, informazioni o programmi*
  - *Diretto a provocare l'interruzione del funzionamento*
- Attesa la genericità della formula, deve ritenersi sussistente il dolo specifico anche se l'agente non si prefigura di commettere personalmente il danneggiamento

La norma precedentemente in vigore non prevedeva il dolo specifico: il fine di danneggiamento era connesso al programma virus

T. Bologna 22 dicembre 2005

Realizza il reato di cui all'art. 615-quinquies c.p. la diffusione del programma cd. Vierika da parte di chi lo ha creato, avendo tale programma per scopo e per effetto l'alterazione di alcune delle funzionalità telematiche di sistemi informatici. "Infatti, gli effetti complessivi creati dai due script di cui è composta Vierika integrano una modificazione dell'ordinario modo di funzionare dei programmi Internet Explorer e Outlook, dal momento che l'invio automatico di e-mail e l'autonoma modifica dei parametri di protezione del browser, senza alcuna conoscenza da parte dell'utente ed in assenza della digitazione degli appositi comandi da parte sua, costituiscono comportamento anormale del sistema

L’esigenza di una nuova incriminazione

Aggiungere un testo con un clic

Forme di danneggiamento

Danneggiamento dell’**hardware**

Danneggiamento del **software**

- Dati
- Programmi

Danneggiamento

Art. 635 c.p.

"Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a 1 anno o con la multa fino a euro 309".

Problema

L'art. 635 c.p. richiede che l'oggetto del danneggiamento sia una **cosa**

- applicabile nel caso di danneggiamento della parte fisica del computer
- problematico se oggetto dell'azione è la componente immateriale (dati e programmi)

Giurisprudenza

La giurisprudenza ha applicato l'art. 635 c.p. anche nei casi di danneggiamento di **dati:**

- nei casi in cui fosse danneggiato anche il supporto
- oppure considerando che il supporto o il computer nel suo complesso erano stati resi almeno parzialmente inservibili

P. Torino, 23 ottobre 1989

" Sono configurabili gli estremi del delitto di danneggiamento nel fatto di chi, mediante una serie di istruzioni indirizzate al calcolatore elettronico, cancelli o alteri alcuni programmi applicativi contenuti in supporti magnetici.

(In particolare è stato osservato che, nella specie, il danneggiamento si è concretato nell'**inservibilità** del sistema informativo, costituito dal connubio indivisibile tra apparecchiature fisiche, programmi e basi di dati)".

Proc. Rep. c/o T.Torino 23.11.1983

(motivi di impugnazione)

"Il comportamento di un tecnico che, recatosi con un pretesto nella sede di una ditta detentrice di un programma elettronico per la gestione della contabilità (software), cancelli definitivamente detto programma lasciando presso la ditta il disco inutilizzabile (hardware), costituisce reato di danneggiamento punito dall'art. 635 c.p., in quanto tale mutilazione comporta l'inservibilità del programma e quindi la parziale inservibilità dell'elaboratore in possesso della ditta. Va pertanto riformata la sentenza di proscioglimento pronunciata dal Pretore, che ha ritenuto non punibile tale comportamento perché attinente ad una entità incorporea."

Cass. S.U. 9 ottobre 1996

" Antecedentemente all'entrata in vigore della l. 23 dicembre 1993, n 547 (in tema di criminalità informatica) che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella **cancellazione di dati** dalla memoria di un computer, in modo tale da rendere necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi dell'art 635 c.p. in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere **inservibile l'elaboratore**"

Esigenze di tutela

L'art. 635 c.p. **non** era comunque applicabile nei casi in cui la cancellazione di dati non avesse comportato l'inservibilità di una cosa corporea

- ipotesi della cancellazione di dati in fase di trasmissione da un elaboratore ad un altro

Il danneggiamento di sistemi informatici

Danneggiamento di sistemi informatici e telematici

Art. 635-bis c.p.

"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili **sistemi informatici o telematici altrui**, ovvero **programmi**, **informazioni** o **dati altrui**, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da 6 mesi a 3 anni".

Particolarità

- danneggiamento di **hardware** e **software**
  - si menzionano anche le 'informazioni'
- ricalca pedissequamente la fattispecie tradizionale
  - stessi eventi dannosi
  - richiede l'altruità del bene 'informatico'

Eventi dannosi

- **Distruzione**
- **Deterioramento**
- **Inservibilità totale o parziale**

Non si menziona la dispersione

Dispersione

Allontanamento dalla sfera di disponibilità dell'avente diritto

- punibile solo se determina l'inservibilità del sistema

Altruità dei beni

Ipotesi problematiche

- *computer* preso in locazione e danneggiato per ritorsione dal proprietario in danno di chi ha il diritto di usarlo
- impossibilità di configurare una proprietà sui dati, in quanto incorporei
  - si deve individuare nel caso concreto chi ha interesse alla integrità dei dati
  - non sempre tale interesse è quello di chi ha la proprietà del supporto

Danneggiamento di hardware

Sanzione **più grave** di quella applicabile in base all'art. 635 c.p.

- occorre un'interpretazione restrittiva
- escluso il danneggiamento di dischi e supporti vergini

Include il danneggiamento di **carte a microprocessore**

Danneggiamento di informazioni

Solo informazioni che presentano un legame funzionale con l'elaboratore:

- destinate ad un processo di elaborazione dati
- provenienti da un processo di elaborazione dati e destinate ad ulteriore elaborazione

Danneggiamento di dati

Anche condotte non punibili con l'art. 635 c.p.

- dati contenuti su supporto esterno
- dati in transito fra due sistemi telematici

Distruzione di dati

Distruzione = **eliminazione definitiva**

- cancellazione, formattazione del supporto, etc.
- i dati non devono essere solo scomparsi alla vista ma esistenti all'interno del sistema
- occorre un effettivo pregiudizio
  - non sussiste se i dati sono facilmente recuperabili da un supporto di riserva o comunque senza alcun dispendio di tempo e denaro

Deterioramento di dati

Deterioramento = **diminuzione in misura apprezzabile del valore del bene**

- virus non distruttivi (graffiti)
- bombe logiche inserite nel programma

Inservibilità dei dati

Inservibilità = **pregiudizio della funzione strumentale del bene**

- alterazione formale dei dati tale da renderne impossibile l'utilizzo (es. cifratura)
- ogni forma di diniego di accesso ai dati da parte del legittimo titolare (es. inserimento di un codice di accesso)

Clausola di sussidiarietà

Ruolo sussidiario della norma incriminatrice, per le ipotesi nelle quali il fatto non integri una diversa fattispecie di reato punita più severamente

ES.:

nel caso di aggressioni a sistemi di pubblica utilità si applicherà esclusivamente l'art. 420 c.p.

Il "nuovo" danneggiamento di dati informazioni e programmi

Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni."

Particolarità

- Nuovi eventi dannosi
  - Cancellazione (di dati)
  - Soppressione (di dati o informazioni)
    - Già riconducibili all'ipotesi della distruzione
  - Alterazione
    - Solo alterazioni dannose
    - Già riconducibile all'ipotesi del deterioramento

Dispersione e inservibilità

- Non si menziona la dispersione nè l'inservibilità
- Punibili solo se riconducibili al deterioramento o all'alterazione
- Ipotesi problematiche:
  - cifratura dei dati
  - inserimento di un codice di accesso

I dati potrebbero non essere direttamente oggetto di intervento

Clausola di sussidiarietà

- Nel caso di aggressioni ad informazioni, dati e programmi di pubblica utilità si applicherà esclusivamente l'art. 635-ter c.p.

Il "nuovo" danneggiamento di sistemi informatici o telematici

Aggiungere un testo con un clic

Danneggiamento di sistemi informatici o telematici

Art. 635-quater

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni."

Modalità di aggressione

- Distruzione
- Deterioramento
- Cancellazione
- Alterazione
- Soppressione

di informazioni, dati o programmi informatici altrui

- Introduzione
- Trasmissione

di informazioni, dati o programmi informatici

(ad es. trasmissione via rete di programmi virus o introduzione di bombe logiche nel sistema)

Danneggiamento dell'hardware

- Mancata menzione del danneggiamento della parte fisica del *computer*
- Applicabilità residuale dell'art. 635 c.p.?
  - giustificabile disparità di trattamento sanzionatorio?

Eventi dannosi

- Distruzione
  - Difficilmente realizzabile con le modalità previste
- Danneggiamento
  - Termine omnicomprensivo
  - Include il deterioramento
  - Anche la dispersione (difficilmente realizzabile)
- Inservibilità
- Ostacolo al funzionamento
  - Ipotesi generalmente già riconducibile all'inservibilità, quantomeno parziale

Clausola di sussidiarietà

- Nel caso di aggressioni a sistemi di pubblica utilità si applicherà esclusivamente l'art. 635-quinquies c.p.

Attentato a sistemi, informazioni, dati e programmi informatici di pubblica utilità

Aggiungere un testo con un clic

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Art. 635 ter c.p.

"Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni."

Bene giuridico tutelato

- Patrimonio?
  - Collocazione sistematica
- Ordine pubblico?
  - Parallelismo con la precedente formulazione dell'art. 420 c.p.

Condotta

- Compimento di atti idonei e diretti al danneggiamento di informazioni, dati e programmi di pubblica utilità.
  - Medesimi eventi dannosi previsti dall'art. 635-bis

Danneggiamento di sistemi informatici o telematici di pubblica utilità

Art. 635-quinquies c.p.

"Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni."

Condotta

- Compimento di atti idonei e diretti al danneggiamento di un sistema di informatico o telematico di pubblica utilità.
  - Medesimi oggetti della condotta ed eventi dannosi previsti dall'art. 635-quater

Modalità del danneggiamento

- Richiamo all'intero fatto previsto dall'art. 635-quater
  - Medesime modalità di danneggiamento (distruzione, deterioramento, cancellazione, alterazione, soppressione, introduzione, trasmissione)
  - Inapplicabilità agli attentati realizzati con altre modalità (es. distruzione fisica del sistema)
    - Applicabilità residuale dell'art. 420 c.p.?

La tutela penale del software

Il quadro normativo previgente

Art. 171 L. 22 aprile 1941, n. 633

Incrimina le condotte di **riproduzione**, **trascrizione**, **diffusione**, **recita in pubblico**, **vendita** e **commercializzazione** delle opere altrui

Problema di analogia:

- il *software* di base è strutturalmente irriducibile all'opera letteraria, in quanto rivolto alla macchina e non all'uomo (Pret. Bologna 24.04.1986)
- Il *software* applicativo non è opera creativa in quanto consiste nella sistemazione di elementi già noti (Pret. Napoli 06.06.1985)

Abusiva duplicazione e commercializzazione di programmi

Art. 171 *bis* L. 22 aprile 1941, n. 633

*Chiunque abusivamente **duplica**, per trarne profitto, programmi per elaboratore o ai medesimi fini **importa**, **distribuisce**, **vende**, **detiene** a scopo commerciale o imprenditoriale o **concede in locazione** programmi contenuti in supporti non contrassegnati dalla Società Italiana degli Autori ed Editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni.*

Le condotte incriminate

- **Abusiva duplicazione**
  - "*abusivamente*": contrarietà della condotta rispetto alla disciplina extrapenale
- ***Importazione***
- ***Distribuzione***
- ***Vendita***
- ***detenzione*** *a scopo commerciale o imprenditoriale*
- ***concessione in locazione***

Il programma come oggetto materiale della tutela

- Insieme compiuto, organico e finalisticamente definito di istruzioni al computer
  - **Originalità**: risultato di creazione intellettuale dell'autore
- Materiale preparatorio per la progettazione del programma?
  - Eccessiva estensione dell'ambito di applicazione della norma
  - Incongruità con determinate condotte (detenzione e locazione)
  - Duplicazione della norma che vieta la rivelazione dei segreti

L'elusione della protezione dei programmi

Art. 171 *bis*, L. 22 aprile 1941, n. 633

*La stessa pena si applica se il fatto **concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale** di dispositivi applicati a protezione di un programma per elaboratori.*

…segue

- Anticipazione della tutela del programma
- Mezzi intesi ad eludere le misure di protezione
  - Solo mezzi fisici
  - Esclusione delle indicazioni e delle informazioni tese allo stesso scopo
- Coincide in parte con il disposto dell'art. 615 *quater* c.p.
  - Si applica comunque la norma in esame, in ragione del trattamento sanzionatorio più rigoroso.

La tutela penale delle banche di dati

Art. 171 *bis* L. 22 aprile 1941, n. 633

*Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE **riproduce**, **trasferisce** su altro supporto, **distribuisce**, **comunica**, **presenta** o **dimostra** in pubblico il contenuto di una banca di dati […] ovvero **esegue l'estrazione o il reimpiego** della banca di dati […], ovvero **distribuisce**, **vende** o **concede in locazione** una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni.*

Le condotte incriminate

- **riproduzione**
  - Su supporto non contrassegnato SIAE
  - Necessariamente “abusiva”, ossia effettuata in violazione del diritto dell’autore della banca dati
  - non è incriminata la riproduzione autorizzata sul supporto non contrassegnato
- **trasferimento** su altro supporto
  - Supporto contrassegnato SIAE
- **distribuzione**
- **comunicazione**
- **presentazione**
- **dimostrazione**

Circostanze aggravanti

Art. 171 *bis* L. 22 aprile 1941, n. 633

La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità