

INDICE - SOMMARIO

I DANNEGGIAMENTI INFORMATICI E TELEMATICI E LE TECNICHE DI INCRIMINAZIONE

Considerazioni introduttive. Pag. 1

Capitolo I

LE LINEE STORICO – EVOLUTIVE: DAI *COMPUTER CRIMES* AI *CYBERCRIMES*

1. La ricerca di una definizione di bene informatico: una breve indagine storica sull'impossibilità di raggiungere l'obiettivo di qualificare il *computer crime* con un concetto unitario. Pag. 9
2. L'atteggiamento del legislatore italiano degli anni Novanta: definizione dei *Computer crimes*. Brevi cenni alla tecnica di formulazione legislativa. 15
3. Il *Cybercrime*: verso una nuova dimensione e concezione di bene giuridico protetto. 18
4. Nuove problematiche dal *cyberspace*: cenni alle questioni di giurisdizione correlate al *Cloud computing*. 26

Capitolo II

LE FONTI SOVRANNAZIONALI: GLI OBBLIGHI D'INCRIMINAZIONE PER I FATTI DI DANNEGGIAMENTO INFORMATICO.

1. Il primo *report* sul *computer crime* OCDE del 1986; le iniziative, coeve, in ambito europeo. Pag. 37
2. Le iniziative del Consiglio d'Europa, in particolare, la Raccomandazione R(89) 9. 43
3. Risoluzione A.I.D.P. sulla criminalità informatica di Rio de Janeiro 1994. 45
4. La Raccomandazione R (95)13 e le altre iniziative del Consiglio d'Europa negli anni Novanta. 47
5. La Convenzione *Cybercrime* di Budapest 2001 ed il rapporto esplicativo. Profili generali e definizioni. 49

INDICE - SOMMARIO

- 5.1 Segue – Profili di diritto sostanziale: i reati cibernetici ‘in senso proprio’ previsti dall’art. 2 CoC - «*Accesso illegale ad un sistema informatico* »- e dall’art. 6 CoC -«*Abuso di apparecchiature*»-. 55
- 5.2 Segue – Profili di diritto sostanziale: i reati cibernetici ‘in senso proprio’ previsti dall’art. 4 CoC - «*Attentato all’integrità dei dati*»- e dall’ art. 5 CoC - «*Attentato all’integrità di un sistema*» -. 61
6. Gli “studi” della Commissione delle Comunità Europee. Dalla Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale e al Comitato delle Regioni (COM/890/2001) - «*Creare una società dell’informazione sicura migliorando la sicurezza delle infrastrutture dell’informazione e mediante la lotta alla criminalità informatica*»- alla proposta di Decisione Quadro del Consiglio, presentata dalla Commissione, e relativa agli attacchi contro i sistemi di informazione (COM(2002)173). 68
7. Le iniziative dell’Unione Europea. La DQ 2005/222/GAI del Consiglio dell’Unione Europea del 4 febbraio 2005, «*Relativa agli attacchi contro i sistemi di informazione*». Profili generali e di diritto sostanziale. 75
8. Gli “studi” della Commissione delle Comunità Europee. Dalla Comunicazione al Parlamento Europeo, al Consiglio e al Comitato delle Regioni (COM/267/07) -«*Verso una politica generale di lotta contro la cybercriminalità*» - al documento COM/448/08 - «*Relazione della Commissione al Consiglio ai sensi dell’art. 12 della DQ 2005/222/GAI*». 79
9. Le iniziative dell’Unione Europea. La Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio dell’Unione Europea del 12 agosto 2013 «*relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio*». 85

Capitolo III

**LA NORMATIVA ITALIANA IN MATERIA DI DANNEGGIAMENTO
INFORMATICO ALLA LUCE DELLA REVISIONE CODICISTICA OPERATA
CON LA LEGGE 23 DICEMBRE 1993, n. 547**

1. I primi casi di danneggiamento informatico e le difficoltà di sussunzione degli stessi entro la categoria tradizionale del danneggiamento di cose.	Pag. 91
2. Profili generali e genesi del danneggiamento informatico.	101
3. L'art. 635- <i>bis</i> c.p.: sulla struttura del reato.	111
3.1. Segue. L'oggetto del reato: sistemi informatici ed 'informazioni'.	117
3.2. Segue. Il concetto di altruità.	122
3.3. Segue. L'art. 392 c.p. ed il nuovo concetto di violenza sulle cose.	124
3.4. Segue. Le condotte punibili.	128
3.5. Segue. L'art. 635- <i>bis</i> , co. 2, c.p. Le circostanze aggravanti.	137
4. Brevi cenni sul rapporto tra l'art. 635- <i>bis</i> c.p. e gli articoli 420 e 615- <i>ter</i> c.p..	139
4.1. Segue. L'art. 615- <i>quinquies</i> c.p. ed il difficile rapporto con l'art. 635- <i>bis</i> c.p.	144
5. Il caso Vierika: un esempio giurisprudenziale oscillante tra accesso abusivo e danneggiamento, nell'ipotesi di diffusione di <i>virus</i> informatici.	150
6. I limiti delle diverse figure di danneggiamento previste dalla l. 547/93 e le esigenze di riforma.	158

Capitolo IV

**LE NOVITÀ INTRODOTTE DALLA L. 48/08 DI RATIFICA ED ESECUZIONE
DELLA CONVENZIONE CYBERCRIME**

1. L' <i>Internet</i> e la rete: i nuovi orizzonti del crimine informatico. Esigenze di riforma o di riformulazione degli illeciti nel campo dell'informatica? ..	163
2. La legge n. 48 del 18 marzo 2008 di ratifica della Convenzione di Budapest. Brevi cenni ai lavori parlamentari e profili introduttivi.	172

INDICE - SOMMARIO

3. Le nuove disposizioni in materia di delitti contro la sicurezza e l'integrità dei dati e dei sistemi informatici 'privati'. L'art. 635-bis c.p. « <i>Danneggiamento di informazioni, dati e programmi informatici</i> ».	176
3.1. Segue. L'art. 635-quater c.p. « <i>Danneggiamento di sistemi informatici o telematici</i> ».	181
3.2. Segue. Il concetto di « <i>Altruità</i> » dei "beni" informatici.	185
3.3. Segue. Le circostanze aggravanti.	190
3.4. Segue. I problemi di concorso fra reati.	191
4. Le nuove disposizioni in materia di delitti contro la sicurezza e l'integrità dei dati e dei sistemi informatici 'pubblici'. In particolare la tecnica di formulazione dei nuovi delitti previsti negli artt. 635-ter, 635-quinquies c.p.	194
4.1. Segue. L'art. 635-ter, co. 1, c.p. « <i>Danneggiamento di informazioni dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità</i> » e l'art. 635-quinquies, co.1, c.p. « <i>Danneggiamento di sistemi informatici e telematici di pubblica utilità</i> »: rilievi critici in ordine alla loro struttura di delitti di attentato.	197
4.2. Segue. L'art. 635-ter, co.2, c.p. « <i>Danneggiamento di informazioni dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità</i> » e l'art. 635-quinquies, co. 2, c.p. « <i>Danneggiamento di sistemi informatici e telematici di pubblica utilità</i> »: rilievi critici in ordine alla loro configurazione come reati (apparentemente) aggravati dall'evento.	203
5. La riformulazione dell'art. 615-quinquies c.p.	206
6. L'esperienza giurisprudenziale più recente.	210

Capitolo V

**L'ATTUAZIONE DELLE FONTI SOVRANNAZIONALI IN SPAGNA.
IL DANNEGGIAMENTO DI DATI E DI SISTEMI INFORMATICI: GENESI ED
EVOLUZIONE DELL'ART. 264 CP E DELL'ART. 197 C.P., FATTISPECIE
PRODROMICA AL DANNEGGIAMENTO INFORMATICO.**

1. Profili generali.	Pag. 215
2. Il <i>Código penal</i> del 1995 ed i dubbi in ordine alla formulazione dell'art. 264.2 CP spag. Prospettive dottrinali.	218
3. Analisi degli elementi della fattispecie prevista dall'art. 264.2 CP spag. .	226
4. L' Art. 197 CP spag., ossia l'accesso ai sistemi informatici e telematici nel <i>Código Penal</i> del 1995. L'irrilevanza penale dell' <i>hacking</i>	233
5. Giurisprudenza. I primi casi di danneggiamento informatico.	235
6. La riformulazione dell'art. 264 ad opera della <i>Ley Orgánica</i> n. 5/10. In particolare, l'Art. 264.1 CP spag.	241
6.1. Segue. L' art. 264.2 CP spag.	253
7. Il nuovo reato di accesso non autorizzato ai dati e ai programmi informatici, fattispecie prevista dall'art. 197.3 CP spag.	256
8. Giurisprudenza. I nuovi casi di danneggiamento informatico.	262
 <i>Considerazioni critiche finali in prospettiva comparata e de lege ferenda.</i>	 Pag. 267
 BIBLIOGRAFIA	 Pag. 281