

## INDICE-SOMMARIO

<i>Prefazione alla prima edizione</i> . . . . .	<i>pag.</i> XXI
<i>Introduzione alla terza edizione.</i> . . . . .	XXVII

### Capitolo primo

LE INIZIATIVE INTERNAZIONALI DI STUDIO E DI RICERCA SULLA VULNERABILITÀ DELLA SOCIETÀ INFORMATIZZATA ED IN TEMA DI CRIMINALITÀ INFORMATICA . . . . .	1
--	---

### Capitolo secondo

LA VULNERABILITÀ DELLA SOCIETÀ INFORMATIZZATA - I SETTORI C.D. CRITICI	
1. Premessa . . . . .	7
2. La difesa militare . . . . .	8
3. La protezione civile . . . . .	14
4. I trasporti . . . . .	14
5. La banca e la borsa . . . . .	15
6. I sistemi di votazione, la sanità, l'istruzione . . . . .	17
7. La previdenza sociale e il fisco . . . . .	21
8. I sistemi elettronici di trasferimento di fondi (c.d. EFTS) . . . . .	22

### Capitolo terzo

IN PARTICOLARE I PROBLEMI DELLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE E LE INIZIATIVE INTERNAZIONALI E NAZIONALI	
1. Definizioni e categorie . . . . .	25
2. Iniziative internazionali . . . . .	26
3. Iniziative italiane di studio sul problema relativo alle infrastrutture critiche in- formatizzate . . . . .	28
4. I compiti del Ministero dell'Interno nei confronti delle infrastrutture critiche informatizzate (art. 7-bis legge 31 luglio 2005, n. 155) . . . . .	29
5. Necessità di diverse iniziative in tema di protezione delle infrastrutture critiche	31
6. Conclusioni e proposte . . . . .	32

Capitolo quarto	
I RISCHI PER ALCUNE INFRASTRUTTURE CRITICHE: «HACKING THE SMART GRID» . . . . .	35
Capitolo quinto	
STUDI, RICERCHE ED INDAGINI STATISTICHE IN TEMA DI CRIMINALITÀ INFORMATICA . . . . .	41
Capitolo sesto	
I DIVERSI APPROCCI SISTEMATICI AL FENOMENO DELLA DELINQUENZA INFORMATICA . . . . .	55
Capitolo settimo	
ALCUNE CATEGORIE DI <i>COMPUTER-CRIMES</i> . . . . .	61
Capitolo ottavo	
MODALITÀ DI COMMISSIONE DEI <i>COMPUTER-CRIMES</i>	
1. <i>Data Diddling</i> (manipolazione dei dati) . . . . .	67
2. <i>Trojan Horse</i> . . . . .	68
3. <i>Salami Techniques</i> . . . . .	68
4. <i>Superzapping</i> . . . . .	68
5. <i>Trap Door</i> (porta a trappola, botola) . . . . .	69
6. <i>Logic Bomb</i> (Bomba logica) . . . . .	69
7. <i>Asynchronous Attacks</i> . . . . .	70
8. <i>Scavenging</i> (raccolta di rifiuti) . . . . .	70
9. <i>Data Leakage</i> . . . . .	71
10. <i>Piggybacking and Impersonation</i> . . . . .	71
11. <i>Simulation and Modeling</i> . . . . .	72
12. <i>Denial of service (DOS)</i> e <i>Denial distribued of service (DDOS)</i> . . . . .	72
Capitolo nono	
LE DIMENSIONI ED I COSTI DEI <i>COMPUTER-CRIMES</i> . . . . .	73
Capitolo decimo	
IL PROFILO PSICOLOGICO DEL <i>COMPUTER-CRIMINAL</i> . . . . .	79

## Capitolo undicesimo

GLI *HACKERS* ALL'ATTACCO DEI COMPUTERS

1. Premessa . . . . .	83
2. I terroristi tecnologici . . . . .	85
3. La tipologia degli «untori informatici». . . . .	88

## Capitolo dodicesimo

I *VIRUS* INFORMATICI E LE LORO IMPLICAZIONI GIURIDICHE

1. I <i>virus</i> e gli altri strumenti dell'attacco informatico: problemi definitivi . . . . .	93
2. Il concetto di «bene informatico» e le norme penali a tutela del patrimonio . . . . .	95
3. Il danneggiamento dei sistemi informatici e le iniziative repressive internazionali . . . . .	97
4. La repressione penale del danneggiamento dei sistemi informatici in vari Paesi. Cenni di diritto comparato . . . . .	98
5. L'uso dei <i>virus</i> e le decisioni delle autorità giudiziarie italiane . . . . .	101
6. Conclusioni . . . . .	106

## Capitolo tredicesimo

## LE VITTIME DELLA CRIMINALITÀ INFORMATICA

1. Le categorie maggiormente vittimizzate. . . . .	109
2. Il comportamento delle vittime. . . . .	110
3. I pericoli di internet: cyber omicidi, cyber suicidi e cyber sex crimes . . . . .	112
4. Le molestie e ingiurie telematiche mediante sms e mms. . . . .	114

## Capitolo quattordicesimo

*STALKING* E *CYBER STALKING* ALL'ITALIANA. . . . . 117

## Capitolo quindicesimo

## CRIMINALITÀ ORGANIZZATA E COMPUTERS . . . . . 127

## Capitolo sedicesimo

LA PROTEZIONE DEI PROGRAMMI INFORMATICI.  
ASPETTI GIURIDICI E RIFLESSI ECONOMICI

1. Premessa . . . . .	131
2. Le conseguenze economiche della pirateria del software: le indagini nei vari Paesi . . . . .	134
USA . . . . .	134
Regno Unito . . . . .	136
Francia . . . . .	137

Italia . . . . .	139
Spagna . . . . .	139
3. I punti di vista delle «software houses» e le opinioni del pubblico sulla repressione della pirateria . . . . .	140
4. Le ricerche dell'OCSE sulle implicazioni economiche della protezione del software . . . . .	142
5. Gli strumenti penalistici per la protezione del software . . . . .	144
a) Leggi penali generali . . . . .	144
b) Leggi sui segreti industriali e commerciali . . . . .	146
c) Leggi sul diritto d'autore . . . . .	155
6. La situazione normativa e giurisprudenziale in Italia . . . . .	170
7. Conclusioni . . . . .	181

#### Capitolo diciassettesimo

#### LA LEGGE ITALIANA N. 547 DEL 1993 IN TEMA DI REPRESSIONE DELLA CRIMINALITÀ INFORMATICA

1. Premessa . . . . .	183
2. L'iter legislativo . . . . .	184
3. I problemi metodologici esaminati dalla Commissione Ministeriale . . . . .	187
4. L'esame delle singole disposizioni dalla legislazione presedente (legge 23 dicembre 1993 n. 547) . . . . .	192
Art. 392 c.p. . . . .	192
Art. 420 c.p. . . . .	193
Art. 491- <i>bis</i> . . . . .	195
Art. 615- <i>ter</i> . . . . .	197
Art. 615- <i>quater</i> . . . . .	198
Art. 615- <i>quinquies</i> . . . . .	199
Art. 616 c.p. . . . .	199
Art. 617- <i>quater-quinquies-sexies</i> . . . . .	200
Artt. 620-621-623 . . . . .	201
Art. 635- <i>bis</i> . . . . .	202
Art. 640- <i>bis</i> . . . . .	203
5. In particolare: le modifiche di alcune norme del codice di procedura penale . . . . .	203
6. Le altre iniziative normative . . . . .	205

#### Capitolo diciottesimo

#### PROFILI PROCEDURALI DELLA LOTTA ALLA CRIMINALITÀ INFORMATICA. ASPETTI NAZIONALI ED INTERNAZIONALI

1. Premessa . . . . .	207
2. L'acquisizione delle prove in area informatica secondo il sistema della legge n. 547 del 1993 . . . . .	209
3. Le intercettazioni delle comunicazioni tra computers . . . . .	211

INDICE-SOMMARIO	XI
4. Problemi interpretativi nell'applicazione degli articoli 266- <i>bis</i> e 268 c.p.p . . . . .	216
5. La competenza dell'autorità giudiziaria italiana in materia di reati informatici transfrontalieri . . . . .	225
6. I nuovi strumenti internazionali di assistenza giudiziaria. . . . .	226
7. Il superamento nell'attività di accertamento dei reati informatici dei mezzi di protezione all'accesso . . . . .	227
8. Le attività delle organizzazioni internazionali nella lotta alla criminalità informatica: regole processuali . . . . .	228
Capitolo diciannovesimo	
L'ANDAMENTO DELLA CRIMINALITÀ INFORMATICA IN ITALIA . . . . .	231
Capitolo ventesimo	
LA SITUAZIONE GIURISPRUDENZIALE IN ITALIA PER QUANTO RIGUARDA LA REPRESSIONE DEI <i>COMPUTER-CRIMES</i>	
1. Premessa . . . . .	235
2. Periodo dal 1970 al 1994 . . . . .	236
3. E dal 1995 al 2002 . . . . .	242
4. La giurisprudenza recente in tema di accesso abusivo all'elaboratore . . . . .	249
Capitolo ventunesimo	
CENNI SULLE LEGGI NAZIONALI IN TEMA DI <i>COMPUTER-CRIMES</i> : IL PANORAMA EUROPEO	
1. Esame sintetico delle normative . . . . .	255
2. Testi di legge allegati . . . . .	263
Capitolo ventiduesimo	
I PROBLEMI GIURIDICI RELATIVI ALLA SICUREZZA INFORMATICA	
1. Premessa . . . . .	287
2. Iniziative in materia di sicurezza informatica delle maggiori organizzazioni internazionali . . . . .	289
3. Gli organismi statali aventi per scopo la sicurezza informatica: panorama internazionale . . . . .	302
4. Le legislazioni nazionali in tema di «computer security» . . . . .	309
5. Cenni sulle ricerche e studi in tema di sicurezza informatica . . . . .	310
6. Sicurezza informatica e protezione dei dati: il panorama internazionale . . . . .	314
7. La sicurezza nei sistemi informatici pubblici: la situazione italiana. . . . .	315
7a. I precedenti storici delle iniziative istituzionali . . . . .	315

7b. Le iniziative del primo Governo Berlusconi in tema di sicurezza informatica nei sistemi pubblici . . . . .	323
7c. La politica del Governo Prodi relativamente alla sicurezza informatica nei sistemi pubblici . . . . .	327
7d. Il CNIPA e la sicurezza nei sistemi informatici pubblici . . . . .	331
7e. Il tramonto del CNIPA . . . . .	337
Capitolo ventitresimo	
LO SPIONAGGIO INDUSTRIALE ED IL «FURTO DI TECNOLOGIA» . . . . .	341
Capitolo ventiquattresimo	
LO SPIONAGGIO COSMICO. IL SISTEMA «ECHELON» . . . . .	349
Capitolo venticinquesimo	
I RIFLESSI GIURIDICI DELLE NUOVE TECNOLOGIE INFORMATICHE . . . . .	359
Capitolo ventiseiesimo	
LE FRODI ONLINE: IL <i>PHISHING</i> E LE SUE VARIANTI.	
1. Il cd. furto di identità personale . . . . .	365
2. Computers zombie, le reti «botnets» e lo spyware . . . . .	369
3. L'evoluzione delle frodi online . . . . .	372
4. Le tipologie di attacco phishing, pharming, vishing . . . . .	374
5. L'inquadramento giuridico del phishing . . . . .	377
Capitolo ventisettesimo	
L'USO DELLO SPAM ED I RELATIVI PROBLEMI GIURIDICI	
1. L'attività delle organizzazioni internazionali in tema di lotta allo spam . . . . .	382
2. La tutela penale, civile ed amministrativa nei confronti delle spam . . . . .	387
Capitolo ventottesimo	
L'USO DELLA REALTÀ VIRTUALE E DEI SISTEMI MULTIMEDIALI NEL PROCESSO PENALE	
1. Premessa . . . . .	391
2. Le applicazioni della realtà virtuale ed il processo penale italiano . . . . .	394

## Capitolo ventinovesimo

LA PROTEZIONE DEI DATI PERSONALI  
ED I PROBLEMI GIURIDICI SORTI A SEGUITO  
DELLA LEGGE N. 675 DEL 31 DICEMBRE 1996

1. Premessa . . . . .	401
2. Le nuove norme . . . . .	402
3. Rilievi e perplessità . . . . .	405
4. L'iter normativo relativo alla creazione della figura del Garante per la protezione dei dati personali . . . . .	410
5. Attività del Garante . . . . .	417
6. Il «day after» delle leggi n. 675 e n. 676 del 1996 . . . . .	418
7. Osservazioni in tema dell'attuale composizione dell'ufficio del garante. . . . .	421

## Capitolo trentesimo

## LE BANCHE DEI DATI IN AMBITO PUBBLICO: PROBLEMI DEFINITORI 425

## Capitolo trentunesimo

## EVOLUZIONE TECNOLOGICA E DIRITTI DELL'INDIVIDUO

1. Premessa . . . . .	427
2. Vita privata, nuove tecnologie e paura del crimine. . . . .	430
3. Problemi posti nel settore della protezione dei dati dalle nuove tecnologie . . . . .	433
a) Telemetria . . . . .	433
b) Mezzi interattivi . . . . .	433
c) Corriere elettronico e posta elettronica . . . . .	433
4. Ordine pubblico e lotta alla criminalità. . . . .	436
5. La sorveglianza elettronica. . . . .	438
6. Il controllo elettronico sul lavoro ed il rispetto della vita privata dei lavoratori . . . . .	442
7. La prigione elettronica . . . . .	445
8. Conclusioni . . . . .	447

## Capitolo trentaduesimo

ANALISI DEI PROFILI PENALI  
DELLA LEGGE SULLA PROTEZIONE DEI DATI PERSONALI

1. Premessa . . . . .	451
2. Le norme penali della legge n. 675: come erano . . . . .	451
3. Le norme penali della legge n. 675 dopo la riforma. Brevi note sulle modifiche delle disposizioni penali della legge n. 675 introdotte dal d.lgs. n. 467 del 28 dicembre 2001 . . . . .	463
4. Considerazioni conclusive . . . . .	466

## Capitolo trentatreesimo

CENNI SUI PROBLEMI GIURIDICI RELATIVI ALL'USO  
DELLE APPARECCHIATURE INFORMATICHE E DI  
TELECOMUNICAZIONE IN AMBIENTE DI LAVORO

- |   |     |
|---|-----|
| 1. La legittimità del controllo della posta elettronica da parte del datore di lavoro. . . . .  | 469 |
| 2. Le Linee Guida del Garante per la protezione dei dati personali per quanto riguarda la navigazione in Internet e l'uso della posta elettronica . . . . . | 481 |
| 3. La direttiva 02/09 del Ministro per la pubblica amministrazione e le tecnologie. . . . .   | 484 |

## Capitolo trentaquattresimo

BREVI CENNI IN TEMA DI RESPONSABILITÀ PENALI CONNESSE  
AL TRATTAMENTO ED ALL'USO DEI DATI SANITARI

- |  |     |
|--|-----|
| 1. Premessa . . . . .  | 491 |
| 2. Misure di sicurezza per la protezione dei dati sanitari. . . . .  | 492 |
| 3. Problematiche penalistiche connesse al consenso per il trattamento dei dati sanitari ed alla loro comunicazione . . . . . | 494 |
| 4. Trattamento dei dati sanitari e responsabilità professionale. . . . .   | 497 |

## Capitolo trentacinquesimo

L'ATTENTATO ALLE TWIN TOWERS. LE REAZIONI NORMATIVE  
NEGLI STATI UNITI E NEI PAESI EUROPEI.  
LORO INCIDENZA IN TEMA DI PROTEZIONE DELLA PRIVACY,  
DI SICUREZZA INFORMATICA E DI REPRESSIONE  
DEI COMPUTER CRIMES

- |  |     |
|--|-----|
| 1. Premessa . . . . .  | 499 |
| 2. Le restrizioni in tema di libertà personale e di protezione dei dati personali . . . . .  | 500 |
| 3. Le reazioni politiche e normative a livello internazionale e nazionale. . . . .   | 504 |
| 4. Innovazioni e modificazioni introdotte in USA dal «Patriot Act» rispetto a leggi preesistenti: in particolare al «Computer Fraud and Abuse Act» . . . . . | 509 |
| 5. L'Homeland Security Act of 2002. . . . .  | 512 |

## Capitolo trentaseiesimo

## INTERNET, TERRORISMO E LOTTA POLITICA ONLINE

- |   |     |
|---|-----|
| 1. L'uso di Internet da parte dei terroristi. . . . . | 515 |
| 2. La lotta politica in rete . . . . .                | 516 |

3. Il piano USA di sorveglianza globale: il TIA (Total Information Awareness System) . . . . .	517
4. Il cyberterrorismo e le iniziative del Consiglio d'Europa . . . . .	520

## Capitolo trentasettesimo

LA REGOLAMENTAZIONE GIURIDICA DI INTERNET  
E L'USO ILLECITO DELLA RETE

1. L'uso illecito di Internet: le iniziative internazionali e nazionali. . . . .	523
1.1. L'Unione Europea . . . . .	523
1.2. L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) . . . . .	526
1.3. Il Consiglio d'Europa . . . . .	527
1.4. Le altre iniziative internazionali . . . . .	527
1.5. Il Gruppo di esperti sul tema «Misuse on International Data Networks» (emanazione del c.d. Carnegie Group) . . . . .	527
1.6. Altre iniziative . . . . .	529
2. I nuovi orizzonti della criminalità: cybermafia e cyberterrorismo. . . . .	531
3. Vecchi e nuovi criminali: gli hackers ed i cyberpunks . . . . .	534
4. Il c.d. cybersquatting. . . . .	539
5. La prevenzione e la repressione degli illeciti commessi mediante l'uso di Internet e di altri servizi telematici interattivi . . . . .	542
6. Il c.d. netstrike . . . . .	543

## Capitolo trentottesimo

## LA PEDOFILIA TELEMATICA: UN NUOVO PERICOLO

1. Premessa . . . . .	547
2. Le recenti iniziative internazionali . . . . .	548
3. USA: il conflitto tra il Congresso e la Corte Suprema . . . . .	554
4. La Convenzione del Consiglio d'Europa: l'art. 9 . . . . .	560
5. La normativa italiana . . . . .	562
6. Osservazioni conclusive e proposte . . . . .	566

## Capitolo trentanovesimo

## I PROBLEMI GIURIDICO-PENALI DEL MILLENNIUM BUG

1. Premessa . . . . .	575
2. Le iniziative legislative estere dirette a prevenire o ridurre l'afflusso di controversie civili . . . . .	577
3. Le iniziative in Italia in ordine ai problemi dell'anno 2000 . . . . .	578
4. I problemi giuridici del mancato adeguamento all'anno 2000 . . . . .	580
5. I possibili reati con riferimento alla fornitura di prodotti informatici con «scadenza» anteriore all'anno 2000. . . . .	581
6. Possibili rimedi per prevenire il verificarsi di un ingorgo giudiziario e per assistere le vittime incolpevoli del millennium bug. . . . .	585

## Capitolo quarantesimo

LA CONVENZIONE DEL CONSIGLIO D'EUROPA  
SULLA CIBERCRIMINALITÀ (BUDAPEST, 23 NOVEMBRE 2001)

1. Lavori preparatori . . . . .	587
2. Cenni generali sul contenuto della Convenzione. . . . .	589
3. Le norme sostanziali . . . . .	591
4. Le disposizioni processuali . . . . .	600
5. La cooperazione internazionale . . . . .	614
6. Le clausole finali. . . . .	622
7. Il Protocollo addizionale alla Convenzione sulla cybercriminalità relativamente alla incriminazione di atti di natura razzista e xenofoba commessi mediante sistemi informatici. . . . .	623

## Capitolo quarantunesimo

LE RECENTI INIZIATIVE DELLA COMUNITÀ EUROPEA  
PER LA LOTTA ALLA CRIMINALITÀ INFORMATICA. . . . .

627

## Capitolo quarantaduesimo

LA LEGGE DI RATIFICA DELLA CONVENZIONE  
A BUDAPEST CONTRO LA CYBERCRIMINALITÀ.  
PROBLEMI APPLICATIVI

1. Premessa . . . . .	631
2. Cenni sull' <i>iter</i> di preparazione del testo del disegno di legge . . . . .	632
3. L' <i>iter</i> normativo del d.d.l. AC n. 2807 . . . . .	634
4. Analisi di alcuni aspetti critici delle norme sostanziali della legge di ratifica . . . . .	641
A) Le modifiche apportate all'art. 420 c.p. già recante il titolo «Attentato ad impianti di pubblica utilità» . . . . .	641
B) Le modifiche all'art. 491- <i>bis</i> c.p. relativo al documento informativo . . . . .	643
C) La falsa dichiarazione o attestazione al certificatore di firma elettronica sulla identità o su qualità proprie o di altri (art. 495- <i>bis</i> ). . . . .	648
D) L'art. 615- <i>quinqüies</i> , relativo alla diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. . . . .	650
5. La frode informatica del certificatore . . . . .	652
6. La normativa in tema di lotta alla pedopornografia informatica e gli equivoci creati dalla relazione al d.d.l. n. 2807 . . . . .	653
7. La modifica al d.lgs. n. 231 del 2001 sulla responsabilità amministrativa degli enti . . . . .	657
8. Il fondo per il contrasto della pedopornografia e per la protezione delle infrastrutture critiche. . . . .	660
9. Il «giallo» delle mancate riserve previste dall'art. 42 della Convenzione. . . . .	662
10. Il rifiuto di consegna della <i>password</i> o dei codici o della chiave crittografica o di qualsiasi informazione relativa ad altra misura di sicurezza. . . . .	665
11. Conclusioni . . . . .	666

INDICE-SOMMARIO	XVII
Capitolo quarantatreesimo	
I PROFILI PROCEDURALI DELLA LEGGE N. 48/2008. . . . .	671
Capitolo quarantaquattresimo	
LA LEGGE N. 48 DEL 2008: I PRIMI NODI AL PETTINE. . . . .	683
Capitolo quarantacinquesimo	
I PROBLEMI TECNICI E GIURIDICI RELATIVI ALL'USO DEL RFID ( <i>RADIO FREQUENCY IDENTIFICATION</i> )	
1. Definizioni e categorie. . . . .	693
2. Settori di applicazione. . . . .	694
3. I Tags RFID e i pericoli per la privacy. . . . .	696
4. Le minacce alla sicurezza. . . . .	698
5. L'attività della Commissione UE nel settore RFID . . . . .	700
Capitolo quarantaseiesimo	
I PROBLEMI TECNICI E GIURIDICI COLLEGATI ALL'USO DEI SISTEMI VOIP ( <i>VOICE OVER INTERNET PROTOCOL</i> )	
1. La vulnerabilità del VOIP e le tipologie di attacco: gli studi e le esperienze in- ternazionali . . . . .	705
2. VOIP E CALEA (Communicative Assistance for Law Enforcement Act). — Cenni sulla situazione in USA . . . . .	716
3. I rischi collegati all'uso del VOIP. . . . .	718
4. Il VOIP ed i problemi delle intercettazioni. . . . .	721
5. I problemi di Skype. . . . .	723
6. Il VOIP e la pubblica amministrazione . . . . .	726
Capitolo quarantasettesimo	
LE TECNOLOGIE BIOMETRICHE TRA ESIGENZE DI «PRIVACY» ED ESIGENZE DI SICUREZZA	
1. Definizioni in tema di biometria. . . . .	737
2. Il mito dell'infallibilità dei sistemi biometrici e della certezza di risultati delle tecniche biometriche . . . . .	739
3. I falsi nel settore delle impronte digitali . . . . .	740
4. La regolamentazione giuridica delle tecnologie biometriche. . . . .	742
5. Le iniziative dell'OCSE nei riguardi delle tecniche biometriche . . . . .	742

## Capitolo quarantottesimo

I SISTEMI DI TRASMISSIONE DI DATI « WIRELESS ».  
PROBLEMI TECNICI E ASPETTI GIURIDICI

Premessa . . . . .	745
1. L'inquadramento giuridico del <i>bluetooth</i> . . . . .	745
2. La vulnerabilità delle reti WI-FI e <i>bluetooth</i> . . . . .	746
3. La normativa amministrativa riguardante l'utilizzo della tecnologia WI-FI. . . . .	753

## Capitolo quarantanovesimo

CONSIDERAZIONI CONCLUSIVE . . . . .	757
-------------------------------------	-----

## ALLEGATI

ALLEGATO A <i>Hacking: cenni sulle radici storiche e culturali del fenomeno e sul suo sviluppo politico</i> . . . . .	763
<i>Allegato n. 1</i> Convenzione del Consiglio d'Europa sulla cybercriminalità (STE n. 185) (aperta alla firma a Budapest il 23 novembre 2001). . . . .	796
<i>Allegato n. 2</i> Recommandation n. R (95) 13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information . . . . .	827
<i>Allegato n. 3</i> Risoluzione del Consiglio dell'UE del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni . . . . .	832
<i>Allegato n. 4</i> Legge federale tedesca per regolamentare le condizioni di base per i servizi di informazione e comunicazione (IuKDG). Legge del 25 luglio 1997. . . . .	838
<i>Allegato n. 5</i> Comité de la politique de l'information, de l'informatique et des communications. Lignes directrice de l'OCDE régissant la politique de cryptographie, 1997 . . . . .	845
<i>Allegato n. 6</i> The Digital Millennium Copyright Act of 1998 - U.S. Copyright Office Summary . . . . .	856
<i>Allegato n. 7</i> United State Code, title 17 . . . . .	873
<i>Allegato n. 8</i> United State Code, title 18 . . . . .	874
<i>Allegato n. 9</i> Décret 2000-405 du 15 Mai 2000. — Décret portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Francia) . . . . .	877
<i>Allegato n. 10</i> Legge del 18 agosto 2000, n. 248. — Nuove norme di tutela del diritto di autore . . . . .	880
<i>Allegato n. 11</i> Raccomandazione del Parlamento europeo sulla strategia intesa a creare una società dell'informazione sicura (2001/2070(COS)) A5-284/2001. . . . .	895
<i>Allegato n. 12</i> Decreto del 2 febbraio 2001. — Modalità di installazione ed uso e descrizione dei tipi e delle caratteristiche dei mezzi elettronici e degli	