

INDICE SOMMARIO

Gli Autori XIII

Parte I ASPETTI TECNICI

CAPITOLO I

LE QUATTRO FASI DELL'ANALISI FORENSE: IDENTIFICAZIONE, ACQUISIZIONE, ANALISI, *REPORTING* di *Giovanni Caria*

1.	Introduzione	3
2.	Identificazione	5
2.1.	<i>Chain of Custody</i>	6
2.2.	Documentazione	7
3.	Acquisizione	8
3.1.	<i>Write blocker</i>	11
3.2.	Acquisizione di un <i>hard drive</i>	12
3.3.	Generazione dei valori di <i>hash</i>	14
4.	Analisi delle prove acquisite.	16
4.1.	Scopo dell'analisi.	16
4.2.	Analisi forense delle immagini.	17
4.3.	Analisi forense di un sito web	19
4.4.	Analisi delle e-mail	19
4.4.1.	Esame del registro di Windows	19
5.	<i>Reporting</i>	25

CAPITOLO II

LE INDAGINI SU DISPOSITIVI DIGITALI di *Katia La Regina*

Sezione I

LA MOBILE FORENSICS

1.	Premessa	27
2.	<i>Mobile forensics e computer forensics</i>	28
3.	Dati potenzialmente significativi	31

4.	Dislocazione dei dati e aree di interesse investigativo	33
5.	Standard di riferimento.	37
6.	Le fasi della <i>mobile forensics</i>	40
6.1.	Preservazione	40
6.2.	Acquisizione.	44
6.3.	Analisi	51
6.4.	<i>Reporting</i>	55

Sezione II

MOBILE DEVICES E PROCEDIMENTO PENALE

1.	Quadro normativo di riferimento.	56
2.	La ricerca della prova. Ispezioni, perquisizioni e sequestri	60
3.	La giurisprudenza sull'ispezione, la perquisizione e il sequestro di telefoni cellulari	62
4.	Un nuovo strumento di ricerca della prova. Il captatore informatico	64
5.	<i>Mobile forensics</i> e accertamenti tecnici irripetibili.	72

Sezione III

CONSULENZA TECNICA D'UFFICIO. REGOLE GENERALI PER LA LIQUIDAZIONE DEI COMPENSI

1.	La determinazione del compenso del CTU.	73
----	---	----

CAPITOLO III

LE *BEST PRACTICES* IN MATERIA DI *COMPUTER FORENSICS*

di *Silvio Marco Guarriello*

1.	Panoramica sulle <i>best practices computer forensics</i>	77
2.	L'immodificabilità della fonte di prova e il metodo scientifico	81
3.	Il sopralluogo informatico	84
4.	Analisi <i>live</i> e <i>post mortem</i> (i perché, pro e contro).	86

Parte II

ASPETTI GIURIDICI

CAPITOLO IV

IL DIRITTO DI FAMIGLIA TRA REATI INFORMATICI, RESPONSABILITÀ GENITORIALE E *DIGITAL FORENSICS*

di *Emilio Tucci*

1.	I reati informatici connessi al diritto di famiglia.	93
1.1.	Accesso abusivo a un sistema informatico o telematico.	95
1.2.	Violazione, sottrazione e soppressione di corrispondenza	97

1.3.	Installazione di apparecchiature atte a intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche.	98
1.4.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	100
1.5.	Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche	101
1.6.	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche	102
1.7.	Danneggiamento di informazioni, dati e programmi informatici.	103
1.8.	Danneggiamento di sistemi informatici o telematici.	104
1.9.	Atti persecutori.	105
1.10.	Diffusione illecita di immagini e video sessualmente espliciti . .	108
1.11.	Molestia o disturbo alle persone.	110
1.12.	Diffamazione	111
1.13.	Interferenze illecite nella vita privata.	113
2.	Le comunicazioni elettroniche tra genitori e figli	115
3.	Software spia e controllo remoto del partner	117
4.	Il controllo tecnologico del minore: tra diritto alla personalità e responsabilità genitoriale	118
5.	La prova digitale in sede penale	120
6.	La prova digitale in sede civile	123
7.	L'acquisizione della prova digitale: profili giuridici e tecnologici. . . .	129

CAPITOLO V

TUTELA DEI DIRITTI E DELLA PRIVACY ONLINE
E OFFLINE DEI SOGGETTI DEBOLIdi *Bruno Tassone e Beatrice Giubilei*

1.	Premessa: dal diritto di essere lasciati soli alla protezione dei dati personali.	135
2.	Il quadro delle fonti sovranazionali	138
3.	Il quadro delle fonti comunitarie e nazionali.	140
4.	I principi del regolamento generale sulla protezione dei dati personali (c.d. GDPR)	149
5.	Informativa e consenso al trattamento del dato	157
6.	I nuovi diritti in ambito privacy	163
7.	I soggetti coinvolti nel "sistema privacy"	172
8.	Privacy e soggetti deboli. Le vittime tipiche	178
9.	Le modalità di protezione dei dati	186
10.	Il <i>data breach</i>	191
11.	La tutela amministrativa	194
12.	La tutela giurisdizionale	199
13.	Le linee del sistema sanzionatorio	201
14.	Le sanzioni amministrative pecuniarie.	203
15.	Le sanzioni penali	206
16.	La responsabilità civile e il risarcimento del danno.	210
17.	Profili afferenti alle investigazioni digitali.	215

CAPITOLO VI

LA REPUTAZIONE DEL MINORE, DELLE VITTIME
E DEI SOGGETTI DEBOLI ONLINEdi *Bruno Tassone e Paolo Cariani*

1. Premessa: onore e reputazione	221
2. Il bilanciamento tra libertà di espressione e diritti costituzionalmente garantiti	225
3. L'identità personale e la reputazione	233
4. L'identità digitale, la persona in rete e la protezione dei dati	237
5. La diffamazione semplice	243
6. La diffamazione aggravata	250
7. Le cause di giustificazione comuni: scriminanti tipiche e ambito di operatività.	252
8. Il diritto di cronaca	255
9. Il diritto di critica	257
10. Il diritto di satira	259
11. La partecipazione ai social network come diritto	260
12. Diffamazione sui social network	263
13. Furto d'identità e management della reputazione.	277
14. Diritto all'oblio: la rimozione dai motori di ricerca.	279
15. Profili risarcitori in ambito civile	290
16. Profili afferenti alle investigazioni digitali.	298

CAPITOLO VII

L'ODIO DOMESTICO, LO SPIONAGGIO
E LA SORVEGLIANZA INTERPERSONALEdi *Piera Di Stefano*

1. Introduzione	305
2. Dal domicilio fisico al domicilio informatico. La tutela della c.d. riservatezza domiciliare.	306
2.1. Premessa	306
2.2. Interferenze illecite nella vita privata (art. 615- <i>bis</i> c.p.).	309
2.3. Accesso abusivo a sistema informatico. Il c.d. reato-mezzo (art. 615- <i>ter</i> c.p.)	317
2.3.1. Rapporti con gli altri reati contro l'inviolabilità del domicilio (artt. 614- <i>quater</i> e 614- <i>quinqüies</i> c.p.)	335
2.3.2. Accesso abusivo e frode informatica (art. 640- <i>ter</i> c.p.)	338
2.3.3. Accesso abusivo e social network	339
2.3.4. Accesso abusivo e violazione di corrispondenza	342
3. La tutela del segreto. I reati contro l'inviolabilità della corrispondenza.	345
3.1. Violazione, sottrazione e soppressione di corrispondenza (art. 616 c.p.)	345
3.2. Violazione della corrispondenza informatica o telematica (art. 616, comma 4, c.p.).	347
3.3. Rivelazione del contenuto di corrispondenza (art. 618 c.p.)	353
3.4. Le tecniche di acquisizione della corrispondenza informatica	354

3.5.	Dati creati con le applicazioni tecnologiche e valore probatorio. Rinvio	358
4.	L'inviolabilità della comunicazione e lo spionaggio domestico. Le intercettazioni tra coniugi	361
4.1.	Intercettazioni e ultimi approdi giurisprudenziali	361
4.2.	I reati contro la riservatezza e la libertà di comunicazione.	374
4.2.1.	Artt. 617 e 617- <i>quater</i> c.p.	374
4.2.2.	Artt. 617- <i>bis</i> e 617- <i>quinquies</i> c.p.	378
4.2.3.	Artt. 617- <i>ter</i> e 617- <i>sexies</i> c.p.	383
4.2.4.	Il nuovo reato di cui all'art. 617- <i>septies</i> c.p.	385
4.3.	L'uso del software spia nell'attività investigativa, tra diritto pretorio e riforme "correttive".	386
4.3.1.	Il captatore informatico nella giurisprudenza di legittimità	386
4.3.2.	Gli interventi riformatori	394
5.	Tecniche di investigazione digitale e reati a mezzo web	403

CAPITOLO VIII

I CRIMINI INFORMATICI A SFONDO SESSUALE

di *Alessia del Pizzo*

1.	I <i>sex crimes</i> nell'era digitale	421
2.	L'abuso sessuale sui minori: cenni descrittivi e normativi	425
2.1.	La tutela internazionale del minore.	431
2.1.1.	I crimini contro la libertà sessuale nella convenzione di Budapest sul <i>cybercrime</i>	439
2.2.	Le azioni di contrasto dell'Unione europea all'abuso e allo sfruttamento sessuale dei minori	442
2.3.	La tutela legislativa penale italiana contro lo sfruttamento sessuale dei minori.	452
2.3.1.	Il decreto Gentiloni: gli obblighi dell'Internet service provider.	462
2.3.2.	La convenzione di Lanzarote e la l. 01.10.2012, n. 172	465
2.3.3.	Il d.lgs. 04.03.2014, n. 39.	471
3.	La dimensione online della pedopornografia: la pedofilia nella rete	471
3.1.	I profili della personalità pedofila	474
3.1.1.	Il cyberpedofilo	477
3.1.2.	Le vittime: dati statistici.	479
4.	I delitti di pornografia minorile: artt. 600- <i>ter</i> , 600- <i>quater</i> e 600- <i>quater.1</i> c.p.	481
4.1.	L'art. 600- <i>ter</i> c.p.	482
4.1.1.	Le condotte previste dall'art. 600- <i>ter</i> , comma 1, c.p.	483
4.1.2.	Le fattispecie disciplinate dagli artt. 600- <i>ter</i> , commi 2, 3 e 4, c.p.	487
4.2.	L'art. 600- <i>quater</i> c.p.: la detenzione di pornografia minorile.	490
4.2.1.	Cenni sulla detenzione e il possesso negli altri ordinamenti	493
4.3.	L'art. 600- <i>quater.1</i> c.p.: la pornografia virtuale	495
5.	Il <i>child grooming</i> : l'adescamento di minorenni	498

5.1.	L'art. 609- <i>undecies</i> c.p.	501
6.	Dalla pedopornografia al <i>sexting</i>	504
6.1.	Le ipotesi di reato associate al fenomeno del <i>sexting</i>	507
7.	<i>Sextortion</i> : il ricatto di natura sessuale	513
8.	<i>Revenge porn</i> : fenomenologia sociale	515
8.1.	Cenni di diritto comparato	519
8.2.	L'introduzione in Italia di una normativa <i>ad hoc</i> : l'art. 612- <i>ter</i> c.p.	520
9.	Le azioni di contrasto ai <i>cybersex crime</i>	526
9.1.	Profili investigativi	527
9.2.	Il CNCPO	530
9.2.1.	L'Unità di analisi dei crimini informatici.	533
9.2.2.	L'Osservatorio per il contrasto della pedofilia e della pornografia minorile	535
9.2.3.	Il Garante per la protezione dei dati personali	537

CAPITOLO IX

IL CYBERBULLISMO

di *Fabrizio Corona*

1.	Il bullismo: lo studio e l'analisi del fenomeno	541
2.	Bullismo e diritto: la Costituzione	544
2.1.	Bullismo e violazione della legge penale.	546
2.1.1.	L'imputabilità del bullo minorenne	547
2.2.	Bullismo e violazione della legge civile	549
2.2.1.	Responsabilità del minore.	550
2.2.2.	Responsabilità dei genitori del minore	551
2.2.3.	Responsabilità della scuola	552
3.	Il bullismo nei vari contesti sociali: dalla scuola alla rete	555
3.1.	Bullismo in rete: il cyberbullismo	558
4.	Analisi del fenomeno del cyberbullismo nel contesto europeo	561
4.1.	Programmi Daphne	561
4.2.	"Needs Assessment and Awareness Raising Programme for Bullying in Schools"	564
4.3.	"Tabby in Internet. Threat Assessment of Bullying behavior Internet" e "Tabby trip in EU"	565
4.4.	Interventi e direttive europee	565
5.	Comparazione europea sul cyberbullismo	567
5.1.	Francia	568
5.2.	Germania	569
5.3.	Regno Unito	570
5.4.	Spagna	571
6.	Progetti nazionali per garantire la sicurezza in rete.	572
7.	Iter normativo preliminare alla l. n. 71 del 2017.	577
8.	Analisi normativa della l. 29.05.2017, n. 71	585
8.1.	Art. 1: i principali reati configurabili nei casi di cyberbullismo	586
8.1.1.	Diffamazione a mezzo Internet	588
8.1.2.	I c.d. "hate speech"	590
8.1.3.	Sostituzione di persona	590
8.2.	Art. 2: le misure di rimedio e prevenzione	592

8.3.	Art. 3 e art. 4: aspetti organizzativi e linee guida di orientamento per la prevenzione e il contrasto in ambito scolastico	593
8.4.	Art. 5: informativa alle famiglie e sanzioni in ambito scolastico.	594
8.5.	Art. 6: rifinanziamento del fondo di cui all'art. 12 della l. 18.03.2008, n. 48	595
8.6.	Art. 7: ammonimento del questore	596
9.	Contenuti illeciti: la responsabilità degli Internet service provider e dei social network	597
10.	I social network e le loro policy.	604
10.1.	I meccanismi di segnalazione a disposizione degli utenti di Facebook.	607
10.2.	Twitter e le differenti tipologie di abusi ricondotte all'interno del fenomeno del cyberbullismo	623
10.3.	La questione dell'anonimato e l'effettiva applicazione delle policy di Ask.fm	630
11.	Gli atti di bullismo in onda su YouTube	639
12.	Le indagini degli inquirenti e le decisioni dei giudici.	657

CAPITOLO X

IL CYBERTERRORISMO

di *Gianpiero Uricchio*

1.	Il terrorismo: origini ed evoluzione	675
1.1.	Il terrorismo di matrice religiosa e l'introduzione del web	680
2.	Esiste il cyberterrorismo?	681
2.1.	Il cyberterrorismo	685
2.2.	Il concetto di cyberterrorismo	687
2.3.	I principi alla base del cyberterrorismo	688
3.	Il crimine informatico o cybercrime	689
3.1.	Rapporti tra cyberterrorismo e cybercrime	690
3.2.	Il diritto penale nel cyberspace	692
4.	Il cyberterrorismo religioso	694
4.1.	Prime strategie di prevenzione del cyberterrorismo	696
5.	Introduzione della policy europea antiterrorismo	696
5.1.	La cybersecurity in Europa.	700
5.2.	Quadro giuridico europeo: cyberspazio e utilizzo dei social media.	702
5.2.1.	Accordi e atti fuori e dentro il web	703
5.3.	Ruolo degli Internet service provider	704
6.	Quali sono le principali minacce cibernetiche?	704
6.1.	Strategie di contrasto all'hacktivismo.	706
7.	Terrorismo e cyberspace	708
7.1.	Obiettivi del cyberterrorismo jihadista e cyberisis	710
8.	L'Italia e la minaccia cibernetica	712
8.1.	Il cyberspazio nella legislazione italiana	715
9.	Cybersecurity e GDPR.	716
9.1.	Internet of Things (IoT)	726
10.	L'intelligenza artificiale per sconfiggere il cyberterrorismo	731
11.	Conclusioni	732

<i>Indice analitico</i>	739
-----------------------------------	-----

