

INDICE

Introduzione	XVII
I Curatori e gli Autori	XIX

Capitolo I

LE INDAGINI: RICERCA E UTILIZZO DELLE PROVE DIGITALI

di Cesare Parodi, Valentina Sellaroli, Salvatore Lombardo, Lorenzo Ghirardi

1. Premessa: la prova digitale	1
1.1. Il concetto di prova digitale	1
1.2. Prova digitale e strumento investigativo digitale: il rilevamento tramite GPS	3
1.3. Documento informatico e sistema informatico	5
1.4. Il protocollo di indagine “standard” per reati commessi sul web	8
2. L’acquisizione della prova digitale	11
2.1. Le indicazioni operative: la perquisizione	11
2.2. Il problema della “macchina accesa”	14
2.3. Perquisizione e cloud	17
2.4. L’accesso alle aree protette	22
2.5. Le copie forensi	23
2.6. L’oggetto dell’acquisizione	27
2.7. In particolare, le “acquisizioni” nei confronti dei giornalisti	31
2.8. L’acquisizione dei file di log	32
2.9. Gli ostacoli all’identificazione in rete	35
2.10. L’acquisizione della prova: deep web e dark web	37
2.11. Le intercettazioni di comunicazioni informatiche e telematiche	38
2.12. L’acquisizione tramite captatore e le indicazioni della riforma in tema di intercettazioni.	43
2.13. L’acquisizione della messaggistica istantanea	52
2.14. Messaggistica e decrittazione	57
2.15. L’acquisizione ex art. 234-bis c.p.p	61
2.16. L’acquisizione prima dell’indagine	68
2.17. Indagini e “internet of things”: gli incidenti stradali	70
3. La conservazione della prova digitale	74
4. L’utilizzazione della prova digitale	77
4.1. Premessa	77
4.2. La valutazione sull’ammissibilità	78

4.3.	Prova informatica e prova scientifica	79
4.4.	Gli interventi “integrativi” nel processo di comprensione	83
4.5.	La valutazione del significato probatorio	84
5.	Gli strumenti di collaborazione internazionale	86
5.1.	L’ordine di indagine europeo	86
5.2.	Le indicazioni su specifici atti di indagine a mezzo OEI	88
5.3.	La Convenzione di Budapest sull’assistenza internazionale e il congelamento dei dati	90
5.4.	In particolare: il sequestro dei siti web: modalità e criticità	93

Capitolo II

I REATI PATRIMONIALI

di Cesare Parodi

1.	La frode informatica	103
1.1.	Premessa	103
1.2.	Gli elementi della fattispecie	104
1.3.	La procedibilità e le ipotesi aggravate	107
1.4.	Rapporto con altre fattispecie	108
1.5.	Momento e luogo di consumazione	109
1.6.	Gli interventi sui programmi di gioco	110
1.7.	La casistica in generale	112
1.8.	Telefonia e attività criminali	113
2.	Il commercio on line tra inadempimento e truffa	115
2.1.	Premessa: un fenomeno socio-economico con risvolti penali	115
2.2.	Truffe on line e minorata difesa	118
2.3.	Gli elementi indicativi della rilevanza penale della condotta	120
2.4.	La valutazione in concreto e i riflessi e sulla procedibilità	122
2.5.	L’indebito utilizzo conseguente alle truffe	124
2.6.	Frodi informatiche e truffe on line: il problema della competenza territoriale	125
3.	L’accesso abusivo a un sistema informatico o telematico	128
3.1.	Premessa	128
3.2.	Gli elementi della fattispecie	129
3.3.	Le caratteristiche del sistema	131
3.4.	Il concetto di “abusività”	132
3.5.	Il luogo di consumazione del reato	136
3.6.	Le ipotesi aggravate	138
3.7.	In particolare: l’operatore di sistema	140
3.8.	La casistica	142
3.9.	In particolare: le caselle di posta	144
4.	La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	145
4.1.	Gli elementi della fattispecie	145
4.2.	Le ipotesi aggravate	148

4.3.	Rapporti con altre fattispecie	149
5.	La diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)	150
5.1.	Le finalità della norma	150
5.2.	Gli elementi della fattispecie	151
5.3.	Rapporti con altre fattispecie	153
5.4.	La casistica	154
6.	L'esercizio arbitrario delle proprie ragioni con violenza informatica	155
6.1.	L'inquadramento della fattispecie	155
6.2.	Il concetto di violenza sulle cose	157
7.	Le frodi assicurative	159
7.1.	Premessa: il fenomeno delle frodi assicurative	159
7.2.	Le frodi tramite siti irregolari	160
7.3.	La qualificazione della condotta e le possibili "precauzioni"	162
8.	Il furto di identità digitale	164
8.1.	Il concetto di identità digitale	164
8.2.	La sostituzione di persona: premessa	166
8.3.	Il furto di identità on line	168
9.	Gli strumenti di pagamento elettronici e telematici	169
9.1.	Premessa: le varie tipologie	169
9.2.	E-payments e m-payments	171
9.3.	Le criticità in tema di sicurezza: phishing e vishing	172
9.4.	Le nuove frontiere dell'illecito: vishing e spear phishing	173
10.	Le commercializzazioni illecite on line	174

Capitolo III

I REATI FAMILIARI E RELAZIONALI

di Valentina Sellaroli

1.	Lo "spionaggio" familiare tra sociologia e diritto	179
1.1.	Premessa	179
1.2.	Le fattispecie astrattamente ravvisabili	180
1.3.	Le interferenze illecite nella vita privata	181
1.4.	La presa di cognizione di comunicazioni telefoniche o informatiche.	183
1.5.	Gli accessi abusivi a un sistema informatico o telematico	184
1.6.	La rilevanza delle condotte illecite e l'utilizzo dei documenti acquisiti...	188
1.7.	... segue: utilizzo e violazioni penali.	190
2.	Gli atti persecutori informatici e telematici	193
2.1.	Premessa	193
2.2.	Lo stalker	195
2.3.	Il delitto di atti persecutori: l'oggetto della tutela.	197
2.4.	La descrizione della condotta: le minacce	198
2.5.	Il delitto di violenza privata	202
2.6.	Il concetto di molestie: premessa	203

2.7.	Le molestie “ sostanziali”	206
2.8.	L’evento del reato	213
2.9.	L’elemento soggettivo del reato	215
2.10.	Il rapporto tra gli atti persecutori e altre fattispecie	216
2.11.	Le ipotesi aggravate.	218
3.	La diffusione illecita di immagini sessualmente esplicite	218
3.1.	Premessa	218
3.2.	Il rapporto tra il revenge porn e altre fattispecie	220
3.3.	L’elemento oggettivo delle fattispecie	223
3.4.	Il problema del consenso	224
3.5.	Le ipotesi aggravate	225
4.	Revenge porn e cyber stalking: problematiche comuni	226
4.1.	La procedibilità.	226
4.2.	La facoltà di arresto	231
4.3.	I nuovi obblighi di cui alla L. n. 69/2019	233
5.	Il cyberbullismo.	235

Capitolo IV

I REATI INFORMATICI IN AMBITO AZIENDALE

di Costantino De Robbio, Francesco Agnino

1.	Premessa: informazioni commerciali e tutela della concorrenza	243
2.	Strumenti informatici e turbata libertà del commercio e dell’industria	247
3.	Accesso abusivo intraziendale: le indicazioni della S.C	249
4.	La tutela dei segreti	255
5.	Tutela dei marchi e segni distintivi	261
6.	Il cybersquatting	268
7.	Furto ed appropriazione indebita di dati informatici	272

Capitolo V

PEDOPORNOGRAFIA E REATI IN AMBITO SESSUALE

di Valentina Sellaroli, Salvatore Lombardo, Lorenzo Ghirardi

1.	La pedopornografia telematica	279
1.1.	Premessa	279
1.2.	La pornografia minorile	282
1.3.	La detenzione di materiale pedopornografico	292
1.4.	L’adescamento e sfruttamento di minori	297
1.5.	La pornografia virtuale.	297
1.6.	Le aggravanti	298
1.7.	La confisca	300
2.	Il contrasto alla pedopornografia	301
2.1.	Le strutture di polizia previste dalla L. n. 269/1998	301

2.2.	Le attività di contrasto “tradizionali”	305
2.3.	La figura dell’agente provocatore	307
2.4.	Gli strumenti di contrasto specifici	310
3.	Le estorsioni a sfondo sessuale	314
3.1.	Approccio su piattaforma social o dating app, registrazione video sessualmente esplicito, ricatto.	314
3.2.	L’estorsione avente a oggetto le riprese della vittima in atteggiamenti sessualmente espliciti	318
3.3.	Approccio verso vittime vulnerabili (minori).	330

Capitolo VI

LA FALSITÀ IN DOCUMENTO INFORMATICO

di Irene Scordamaglia

1.	L’art. 491-bis c.p.	323
1.1.	Le ragioni dell’introduzione della norma e le sue vicende modificative.	323
1.2.	La natura della norma.	325
2.	La nozione di documento informatico.	328
2.1.	Documento tradizionale e documento informatico.	328
2.2.	Le varie figure di documento informatico	329
3.	Gli interventi novellatori sull’art. 491-bis c.p.	332
4.	L’efficacia probatoria del documento informatico	334
4.1.	L’efficacia probatoria del documento informatico nella giurisprudenza civile: cenni.	341
4.2.	L’efficacia probatoria del documento informatico nella giurisprudenza penale di legittimità.	343
5.	L’interpretazione dell’art. 491-bis c.p. nella formulazione vigente	346
6.	La falsità materiale e la falsità ideologica in documento informatico.	348
7.	Il falso in atto pubblico informatico	353
8.	Il falso informatico in certificazione o autorizzazione amministrativa	357
9.	Conclusioni	358

Capitolo VII

I REATI IN TEMA DI COMUNICAZIONI

di Claudio Orazio Onorati, Maria Sofia Cozza

1.	Corrispondenza telematica e comunicazione telematica nell’attuale disciplina. Funzione dell’art. 623-bis c.p	361
1.1.	Inquadramento della corrispondenza telematica e della comunicazione telematica nell’attuale disciplina.	361
1.2.	La tutela della casella di posta elettronica	373
2.	Violazione, sottrazione e soppressione di corrispondenza “informatica”	378
2.1.	Introduzione alla norma. Collocazione sistematica e bene giuridico tutelato	378

2.2.	Condotte incriminate	383
2.3.	Elemento soggettivo	384
2.4.	Il secondo comma: la condotta di rivelazione e le cause di non punibilità	384
3.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	386
3.1.	Introduzione alla norma. Collocazione sistematica	386
3.2.	Bene giuridico tutelato	390
3.3.	Le condotte del primo comma.	393
3.4.	Intercettazione	394
3.5.	Le modalità fraudolente.	397
3.6.	Impedimento e interruzione.	399
3.7.	La condotta di rivelazione di cui al secondo comma.	401
3.8.	Elemento psicologico del reato.	403
3.9.	Tentativo.	406
3.10.	Circostanze aggravanti.	406
3.11.	L'operatore di sistema.	409
3.12.	Casistica	410
4.	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	411
4.1.	Introduzione alla norma. Collocazione sistematica e condotte incriminate	411
4.2.	Casistica	414
5.	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche	417
5.1.	Introduzione alla norma. Collocazione sistematica e condotte incriminate	417
5.2.	Le forme più comuni di "intrusione informatica"	419
5.3.	Casistica	423
6.	Diffusione di riprese e registrazioni fraudolente	425
6.1.	Collocazione sistematica e bene giuridico	425
6.2.	Condotte incriminate e soggetto agente	427
6.3.	Elemento soggettivo	431
6.4.	Le cause di non punibilità.	431
6.5.	Rapporti con altre fattispecie di reato: Diffamazione (595 co. 3 c.p.).	432
6.6.	Rapporti con altre fattispecie di reato: Interferenze illecite nella vita privata (615-bis c.p.).	433
6.7.	Rapporti con altre fattispecie di reato: Diffusione illecita di immagini o video sessualmente espliciti (revenge porn) — art. 612-ter c.p.	434
7.	Rivelazione del contenuto di documenti informatici segreti	436
7.1.	Introduzione alla norma. Collocazione sistematica e bene giuridico tutelato.	436
7.2.	Gli elementi costitutivi della fattispecie	437
7.3.	Le cause di non punibilità	441
7.4.	L'art. 623-bis c.p. e sue applicazioni pratiche	442

Capitolo VIII**IL RICICLAGGIO E L'AGGIOTAGGIO TELEMATICO**

di Cesare Parodi, Salvatore Lombardo, Lorenzo Ghirardi

1.	La “rete” e il riciclaggio.	445
1.1.	Le indicazioni generali del D.Lgs. n. 231/2007	445
1.2.	Le possibilità di riciclaggio online	449
1.3.	Le indicazioni del D.Lgs. n. 231/2007 in tema di servizi di gioco.	452
1.4.	Riciclaggio e traffico telefonico	454
2.	Il riciclaggio derivante dal “man in the middle”	455
2.1.	Premessa: il fenomeno “man in the middle”	455
2.2.	Le criticità investigative e la qualificazione dei fatti	457
3.	Tecnologia blockchain, monete virtuali e riciclaggio	461
3.1.	Premessa.	461
3.2.	La tecnologia blockchain.	462
3.3.	Le cripto valute	465
3.4.	Cripto valute: natura giuridica e ruolo nel mercato.	467
3.5.	Monete virtuali e riciclaggio: premessa	469
3.6.	Valute virtuali e disciplina antiriciclaggio il D.Lgs. n. 90/2017	471
3.7.	Il recepimento della Direttiva 2018/843/UE: il D.Lgs. n. 125/2019	474
3.8.	Le modalità di sequestro delle valute virtuali	476
4.	L'aggiotaggio “telematico”	479
4.1.	Premessa: i valori finanziari e le comunicazioni telematiche	479
4.2.	Il delitto di aggiotaggio ex art. 2637 c.c.	481
4.3.	L'aggiotaggio telematico: problemi interpretativi	484

Capitolo IX**LA DIFFAMAZIONE A MEZZO WEB**

di Eugenio Albamonte

1.	Premessa.	487
2.	La responsabilità penale dei media di comunicazione on line	489
2.1.	Principi generali	489
2.2.	I quotidiani e le testate giornalistiche on line.	490
2.3.	La responsabilità degli internet service provider e dei gestori di piattaforme web	495
2.4.	I blog.	498
2.5.	La responsabilità derivante dalla pubblicazione di contenuti sui social network	500
3.	Le scriminanti e la loro applicazione alle comunicazioni tramite piattaforme web e social network.	504
3.1.	L'operatività delle scriminanti.	504
3.2.	Il diritto di critica sui social network e nelle piattaforme commerciali.	509
3.3.	La verità del fatto, il citizen journalism e le fake news.	511

- 3.4. L'interesse generale e il diritto all'oblio. 516
 3.5. La continenza verbale, il linguaggio dell'odio e il body shaming. 518

Capitolo X

LA TUTELA DEL DIRITTO D'AUTORE IN AMBITO INFORMATICO/TELEMATICO

di Simona Lavagnini

1. La tutela dei programmi per elaboratore. 523
 1.1. Alcune nozioni preliminari: Il software fra diritto d'autore, segreto e brevetto 523
 1.2. La tutela del software come opera dell'ingegno 524
 1.3. Le licenze d'uso: le formule tradizionali (a tempo illimitato e con unico pagamento iniziale) e i relativi illeciti. 526
 1.4. La teoria del software usato e l'esaurimento del diritto di distribuzione. 529
 1.5. I contratti open source. 532
 1.6. Le nuove forme di messa a disposizione del software e conseguenti nuovi illeciti 533
 1.7. Il contrassegno ex art. 181-bis l.a., la dichiarazione identificativa sostitutiva e le esenzioni 534
 1.8. Le misure tecnologiche di protezione. 539
 2. La duplicazione abusiva. Software e licenza d'uso. 540
 2.1. La fattispecie penale - art. 171-bis l.a. 540
 2.2. L'abusività, con particolare riguardo al regime delle eccezioni e ai rapporti contrattuali 541
 2.3. La condotta di duplicazione 543
 2.4. Le condotte di importazione, distribuzione, vendita, concessione in locazione; la condotta di detenzione e lo scopo commerciale o imprenditoriale. 546
 2.5. Il dolo specifico dello scopo di profitto 547
 2.6. La presenza/assenza del contrassegno 550
 2.7. L'elusione delle misure tecniche di protezione (unicità del fine) 551
 2.8. Altre condotte 552
 3. La tutela delle banche dati - Il concetto di "banca dati" - Le violazioni 553
 3.1. Alcune nozioni preliminari - Le banche di dati protette come opere dell'ingegno ex art. 1 l.a. 553
 3.2. Le banche di dati oggetto di diritto sui generis ex art. 102-bis l.a. 558
 3.3. Le banche di dati non protette. 561
 3.4. La fattispecie penale: il fine di profitto e il contrassegno SIAE - rinvio. 562
 3.5. Le condotte sanzionate in relazione alle banche di dati opere dell'ingegno. 562
 3.6. Le condotte sanzionate in relazione alle banche di dati oggetto di diritto sui generis: estrazione o reimpiego di dati in violazione degli artt. 102-bis e 102-ter l.a. 565
 4. La tutela delle opere musicali, cinematografiche, letterarie e multimediali. 568
 4.1. Alcune nozioni preliminari 568

4.2.	Gli illeciti commessi online: fenomenologia delle ipotesi più ricorrenti (peer-to-peer, siti pirata, cyber locker, stream ripping, social networks)	573
4.3.	Gli intermediari e la responsabilità	578
4.4.	La fattispecie penale: l'uso non personale, il fine di lucro, l'abusività delle condotte	583
4.5.	Le condotte del primo comma	584
4.6.	Le condotte del secondo comma	586
4.7.	L'art. 171-quater l.a.	588
5.	La tutela del settore televisivo	590
5.1.	Gli illeciti in campo televisivo: fenomenologia, con particolare riguardo alle IPTV abusive	590
5.2.	Le condotte illecite	591

Capitolo XI

I DANNEGGIAMENTI INFORMATICI

di Ivan Salvadori

1.	Premessa	595
2.	Ambito e scopo della trattazione	598
3.	La sicurezza informatica	599
4.	I danneggiamenti di dati e di sistemi informatici "privati"	601
4.1.	Il danneggiamento di dati e di programmi informatici.	601
4.2.	L'oggetto materiale del reato	604
4.3.	L'altruità dei dati e dei programmi informatici	606
4.4.	L'elemento soggettivo	607
4.5.	Momento consumativo e tentativo	607
4.6.	Il danneggiamento di sistemi informatici o telematici.	608
4.7.	L'oggetto materiale del reato	610
4.8.	L'elemento soggettivo	611
4.9.	Momento consumativo e tentativo	611
5.	I danneggiamenti di dati e di sistemi informatici "pubblici"	611
5.1.	I delitti di attentato a dati e sistemi informatici "pubblici"	611
5.2.	L'oggetto materiale del reato	613
5.3.	Elemento soggettivo	613
5.4.	Momento consumativo e tentativo	613
5.5.	Il danneggiamento di dati e di sistemi informatici "pubblici"	614
5.6.	L'oggetto materiale del reato	614
5.7.	L'elemento soggettivo	615
5.8.	Momento consumativo e tentativo	615
6.	La diffusione di apparecchiature dirette a danneggiare dati o sistemi informatici	615
6.1.	L'oggetto materiale del reato	617
6.2.	L'elemento soggettivo	617
6.3.	Momento consumativo e tentativo	617
7.	Trattamento sanzionatorio e circostanze aggravanti	618

8.	I rapporti con altri reati	620
9.	Responsabilità amministrativa degli enti	621

Capitolo XII

INFORMATICA E TUTELA DELLA RISERVATEZZA

di Giuseppe Vaciago, Nicole Monte

1.	Introduzione: GDPR e reati a tutela della riservatezza	623
2.	Dati personali, trattamento e valore economico dei dati personali	628
3.	Titolare del trattamento dei dati personali e responsabile. Principio di accountability e posizione di garanzia	633
4.	Art. 167 D.Lgs. 196/2003 - Trattamento illecito di dati personali: la disciplina previgente e l'interpretazione della Cassazione nel caso Google vs. Vividown	640
5.	Art. 167 D.Lgs. 196/2003 e sanzioni penali nel GDPR	649
5.1.	Le nuove fattispecie previste dall'art. 167 D.Lgs. 196/2003: le principali modifiche	651
5.2.	L'elemento soggettivo del reato: i destinatari del precetto	654
5.3.	La condotta perseguita: gli obblighi violati	656
5.4.	Successioni di leggi penali nel tempo: continuità normativa nel reato di trattamento illecito	658
5.5.	Le fattispecie di reato relative al trattamento "su larga scala"	661
6.	Art. 167 D.Lgs. 196/2003 e art. 615-ter codice penale: concorso tra reati	663
7.	Fattispecie penali in materia di comunicazioni al Garante	666
7.1.	Inosservanza di provvedimenti del Garante: punti in comune con il reato 168 D.Lgs. 196/2003	668
8.	Il rapporto tra l'Autorità Garante per la Protezione dei Dati Personali e l'Autorità Giudiziaria	669
9.	Il contesto europeo in materia di protezione dei dati in ambito di polizia e di giustizia penale	671
9.1.	La Direttiva 2016/680/UE di diritto dell'UE sulla protezione dei dati in ambito di polizia e giustizia penale ed il recepimento in Italia con il D.Lgs. 51/2018	673
10.	Le norme sul controllo a distanza previste dallo Statuto dei lavoratori	678
11.	Riservatezza e tecnologia: conclusioni conclusive	680

Capitolo XIII

DATA RETENTION E GIUSTIZIA PENALE IN ITALIA

di Roberto Flor

1.	Introduzione: le fonti della c.d. data retention	683
2.	Data retention e contesto europeo: un excursus "storico" (alea iacta est)	685
3.	Law in the book: l'interpretazione dell'art. 132 codice privacy alla luce delle fonti europee	691

3.1.	Primo rilievo: i tempi di conservazione dei dati di traffico telefonico e telematico	691
3.2.	Secondo rilievo: le modalità di acquisizione dei dati di traffico telefonico e telematico e, in particolare, l'intervento del Pubblico Ministero	692
3.3.	Terzo rilievo: la « finalità di accertamento e repressione dei reati »	694
3.4.	Osservazioni critiche	695
4.	Law in action: i più recenti orientamenti giurisprudenziali riguardanti l'acquisizione dei dati di traffico telefonico o telematico	697
4.1.	Gli orientamenti "salvifici"	697
4.2.	La parola alla difesa	700
5.	Bene iudicat qui bene distinguit. Quali prospettive?	706

Capitolo XIV

CYBERCRIME E DIRITTO PENALE

di Lorenzo Picotti

1.	Rivoluzione cibernetica e diritto penale	709
2.	Dai Computer crime ai Cybercrime: la criminalità nel Cyberspace	712
3.	Il web interattivo ed il doppio ruolo degli utenti autori e vittime di reati cibernetici: nuovi beni giuridici e diritti fondamentali da proteggere penalmente	716
4.	Osservazioni conclusive: necessità di adeguamento delle categorie del diritto penale e di potenziamento delle posizioni di garanzia nel Cyberspace	719
	Indice analitico	725

